71035800

Mercury®

制 造 商: 深圳市美科星通信技术有限公司
公司地址: 深圳市深南大道高新技术产业园区
深圳市清华大学研究院**B301**
网　　址: http://www.mercurycom.com.cn

Mercury®

水星MR904B

双 WAN口 网 吧 专 用 宽 带 路 由 器

用 户 手 册



Rev: 1.0.0

商标、版权声明

Mercury® 为深圳市美科星公司的注册商标。本产品的所有组成部分，包括配件和软件在内，其版权都归深圳市美科星公司所有，未经深圳市美科星公司许可，不得任意仿制、拷贝、誊抄或转译。本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知，可随时查阅我们的万维网页 http://www.mercurycom.com.cn。

目　　录

物 品 清 单

请您小心打开包装盒，里面应有以下配件:

- 一台MR904B路由器
- 一根电源线
- 一本用户手册
- 一张保修卡

如果发现有配件短缺或损坏的情况，请及时和当地经销商联系。

第1章 用 户 手 册 简 介

首先感谢您购买MR904B双WAN口网吧专用宽带路由器！MR904B双WAN口网吧专用宽带路由器是专为满足小型企业、网吧用户需求而设计的，它集高性能、高安全、多管理功能于一身，为您提供高价值的网络连接。它配置简单，无需专业人员即可按照本手册安装配置。

在您准备安装使用本产品之前，请先仔细阅读本手册，以便全面利用本产品的所有功能。

1.1 用途

本手册的用途是帮助您熟悉和正确使用MR904B双WAN口网吧专用宽带路由器。

1.2 约定

本手册中所提到的路由器，如无特别说明，系指MR904B双WAN口网吧专用宽带路由器，下面简称为MR904B。

本手册采用的图片中都配有相关参数，实际产品的配置界面并没有提供，这些参数主要是为您正确设置参数提供参考，您可以根据实际需要选择是否设置或修改这些参数。

1.3 用户手册概述

第1章：用户手册简介。

第2章：产品概述。简述路由器的主要特性和规格。

第3章：硬件安装。帮助您进行路由器的硬件安装。

第4章：快速安装指南。帮助您配置路由器的基本网络参数。

第5章：配置指南。帮助您配置路由器的高级特性。

附录A：FAQ。

附录B：TCP/IP的详细设置。

第2章 产品概述

2.1 产品简介

MR904B双WAN口网吧专用宽带路由器采用Intel IXP网络专用处理器，基于Intel XScale技术，多CPU分布式处理，性能优越；同时采用六层PCB，1U钢壳，并内置电源模块，充分保证了整机的稳定可靠。

MR904B具有两个WAN口，能够同时进行数据转发，加强了数据包的转发功能。它除了包含所有宽带路由器的常用功能外，还支持攻击防护、基于IP的QoS、单机连接数控制、IP与MAC绑定、端口监控以及配置文件备份/导入等特别适合企业、网吧应用的功能。

支持ISP均衡控制功能，有效利用双WAN口，提高了访问网站的速度。提供攻击防护功能，有效提高网络可靠性。支持内/外部攻击防范，提供扫描类、DoS类、可疑包和含有IP选项的包等攻击保护，能侦测及阻挡IP地址欺骗、源路由攻击、IP/端口扫描、DoS等网络攻击，有效防止Nimda、冲击波、木马等病毒攻击，为企业、网吧提供可靠的安全保障。

基于IP、端口的QoS，可配置单机带宽和连接数，有效防止用户使用P2P等特殊应用过度占用网络资源，让网络游戏更顺畅。可将企业或网吧划分为不同的工作区，设置不同的带宽、连接数，保证特殊分区、特殊应用的服务质量，方便企业网络管理，可实现网吧分区收费。同时提供连接数列表，详细显示各IP地址当前占用的连接数，帮助网管员轻松掌握网络资源分配。

支持IP与MAC绑定，有效防范ARP攻击。ARP攻击频繁发生，会使整个网络陷于瘫痪，影响企业、网吧网络的正常运营。IP与MAC地址绑定功能，强制IP与MAC地址一一对应，同时不能轻易更改，可有效防范ARP攻击。

支持端口镜像，便于网络监控。网吧传输的数据可按要求复制到监控端口，满足公安部门的网吧监控要求，也为分析、解决网络问题提供了参考数据。支持配置备份与导入，可将配置文件保存到电脑，需要复位路由器时，可导入配置文件，缩短配置时间。

MR904B双WAN口网吧专用宽带路由器专为满足企业、网吧用户需求而设计，提供全中文Web配置界面，配置简单，支持免费软件升级功能，能够全面满足企业、网吧用户对高性能、多功能、高可靠性、高安全性的需求。

2.2 特性和规格说明

2.2.1 主要特性

- 支持TCP/IP，DHCP，ICMP，NAT，PPPoE，SNTP，HTTP，DNS等协议
- 提供2个WAN口3个LAN口，10/100Mbps自适应，支持端口自动翻转（Auto MDI/MDIX）
- 支持基于IP或基于端口的QoS设置，可限制单机带宽
- 支持流量均衡控制、ISP均衡控制、均衡策略功能
- 内置简单管理交换机，支持端口带宽控制、VLAN设置和端口镜像等功能
- 支持VPN Pass-through、UPnP和DDNS
- 支持虚拟服务器、特殊应用程序、DMZ主机和静态路由等功能
- 支持连接数设置，可限制单机连接数
- 内建防火墙，支持IP地址过滤、域名过滤、MAC地址过滤
- 提供攻击防护，可对网络攻击和病毒攻击进行防范
- 支持IP与MAC地址绑定，有效防范ARP攻击
- 支持MAC地址修改和克隆
- 提供系统日志功能，支持配置文件备份与载入
- 支持流量统计和IP地址转换表查看功能
- 支持Web和远程管理，全中文配置界面，支持Web软件升级
- 内置电源，1U钢壳，可装19英寸标准机架，工业级设计

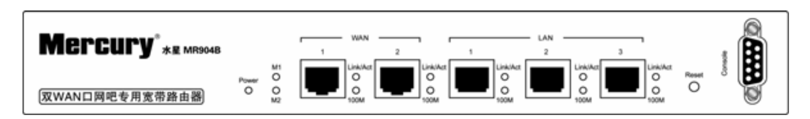
2.2.2 规格

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS
端口	LAN口	3个10/100M自适应RJ45端口（Auto MDI/MDIX）
	WAN口	2个10/100M自适应RJ45端口（Auto MDI/MDIX）
网络介质		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
LED指示	LAN/WAN口	Link/Act（连接/工作）、100Mbps（速度）
	其它	Power（电源）、M1/M2（系统状态指示灯）
外形尺寸(L x W x H)		294mm x 180mm x 44mm
使用环境		工作温度：0ºC 到 40ºC
		存储温度：-40ºC 到 70ºC
		工作湿度：10% 到 90% RH不凝结
		存储湿度：5% 到 90% RH不凝结
电源及功耗		输入：100-240VAC，50/60Hz
		功耗：最大5.6W

第3章 硬件安装

3.1 面板布置

3.1.1 前面板



➢ **Reset:** 复位按钮。关闭电源，按住此按钮，然后打开电源，约过3秒钟，M1，M2指示灯同时闪烁后，可松开按钮，待路由器启动后，其配置将恢复到出厂默认值。

 注意:

在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

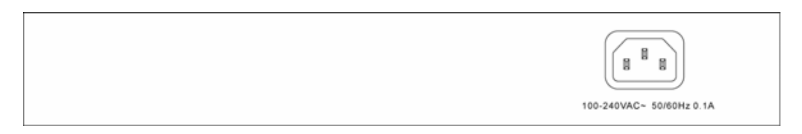
➢ 指示灯:

指示灯	描述	功能	备注
POWER	电源指示灯	常亮表示系统正在运行	
M1	系统状态指示灯	常亮表示系统有故障	M1,M2灯同时闪烁，表示系统正在恢复出厂设置
M2	系统状态指示灯	闪烁表示系统正常	
		常亮或常灭表示系统不正常	
Link/Act	广域网和局域网状态指示灯	常亮表示相应端口已正常连接	
		闪烁表示相应端口正在进行数据传输	
100M	广域网或局域网速度指示灯	常亮表示相应端口位于100M工作模式	
		不亮表示相应端口位于10M工作模式	

➢ **WAN:** 2个广域网端口(RJ45)。连接xDSL/Cable Modem或以太网。

➢ **LAN:** MR904B提供3个局域网端口(RJ45)，计算机、集线器/交换机等通过这些端口连入局域网。

3.1.2 后面板



- **电源插孔：**这个插孔供您插接电源。


注意:

电源规格为：100-240VAC，50/60Hz，如果使用不匹配的电源，可能会导致路由器损坏。

3.2 系统需求

- 宽带Internet服务（接入方式为xDSL/Cable Modem或以太网）
- 具有以太网RJ45连接器的调制解调器（直接接入以太网时不需要此物件）
- 每台PC的以太网连接（网卡和网线）
- TCP/IP网络软件（Windows 95/98/ME/NT/2000/2003/XP/Vista自带）
- Internet Explorer 5.0 或更高版本

3.3 安装环境

安装环境要求:

- 将路由器水平放置
- 尽量将路由器放置在远离发热器件处
- 不要将路由器置于太脏或潮湿的地方

路由器推荐使用环境:

- 温度：0 ºC ~ 40 ºC
- 湿度：5% ~ 90%RH，无凝结

3.4 硬件安装步骤

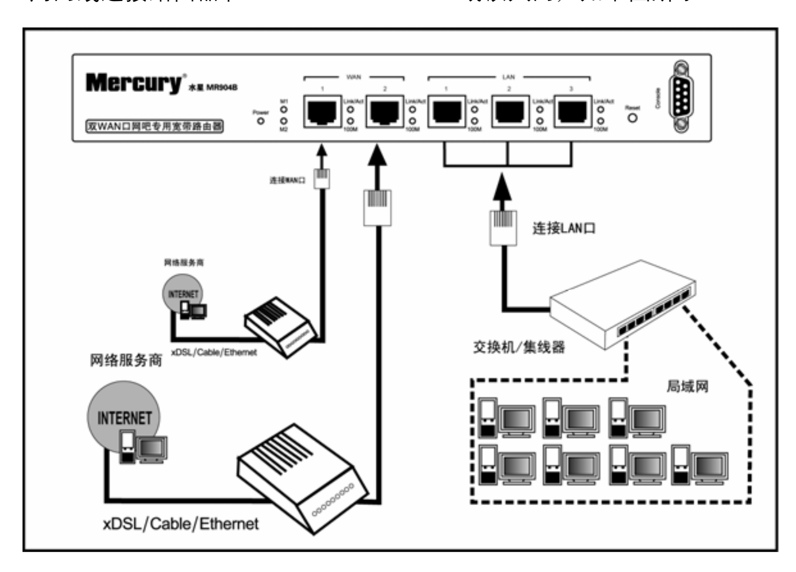
在安装路由器前，我们希望您已经能够利用您的宽带服务在单台计算机上成功上网。如果您单台计算机上宽带网有问题，请先和您的网络服务商（ISP）联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装您的路由器。切记安装时拔除电源插头，保持双手干燥。

1 建立局域网连接

用一根网线连接路由器的LAN口和局域网中的集线器或交换机，如下图3.3所示。您也可以用一根网线将路由器与您的计算机网卡直接相连。

2 建立广域网连接

用网线连接路由器和xDSL/Cable Modem或以太网，如下图所示。



3 连接电源

将电源连接好，路由器将自行启动。

第4章 快速安装指南

要正确使用路由器，您必须合理配置网络。下面以Windows XP为例，讲述具体配置过程。如果只进行基本配置，您只需阅读本章内容；如果要进行高级配置，请继续阅读第五章内容。

4.1 建立正确的网络设置

路由器默认IP地址是192.168.1.1，默认子网掩码是255.255.255.0。这些值可以根据您的实际需要而改变，但本用户手册上将按默认值说明。

首先请将您的计算机接到路由器的局域网端口，接下来您可以使用两种方法为您的计算机设置IP地址。

➢ **方法一**：**手动设置IP地址。**

- 设置您计算机的TCP/IP协议。如果您已经正确设置完成，请跳过第一步。
- 设置您计算机的IP地址为192.168.1.xxx（xxx范围是2至254），子网掩码为255.255.255.0，默认网关为192.168.1.1。

➢ **方法二**：**利用路由器内置DHCP服务器自动设置IP地址。**

- 设置您计算机的TCP/IP协议为“自动获取IP地址”。
- 关闭路由器和您的计算机电源。
- 打开路由器电源，然后再启动您的计算机。
- 这样路由器内置DHCP服务器将自动为您的计算机设置IP地址。

在设置好TCP/IP协议后，您可以使用Ping命令检查您的计算机和路由器之间是否联通。下面的例子为一个在Windows XP环境中，执行Ping命令，操作步骤如下:

首先请您点击桌面的“开始”菜单，再选择“运行”选项，并在随后出现的运行输入框内输入cmd命令，然后回车或点击“确认”键即可进入下图所示界面。

最后在该界面中输入命令Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为:

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

那么恭喜您！您的计算机已与路由器成功建立连接。如果屏幕显示为:

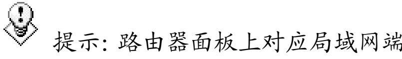
```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，您可以按照下列顺序检查:

1) **硬件连接是否正确?**



提示: 路由器面板上对应局域网端口的 Link/Act 指示灯和您计算机上的网卡灯必须亮。

2) **您的计算机的 TCP/IP 设置是否正确?**



提示: 如果路由器的 IP 地址为 192.168.1.1，那么您的计算机 IP 地址必须为 192.168. 1.xxx（xxx 范围是 2~254）。

4.2 快速安装指南

本产品提供基于浏览器（Internet Explorer或Netscape Communicator）的配置界面，这种配置方案适宜于任何MS Windows，Macintosh或UNIX平台。

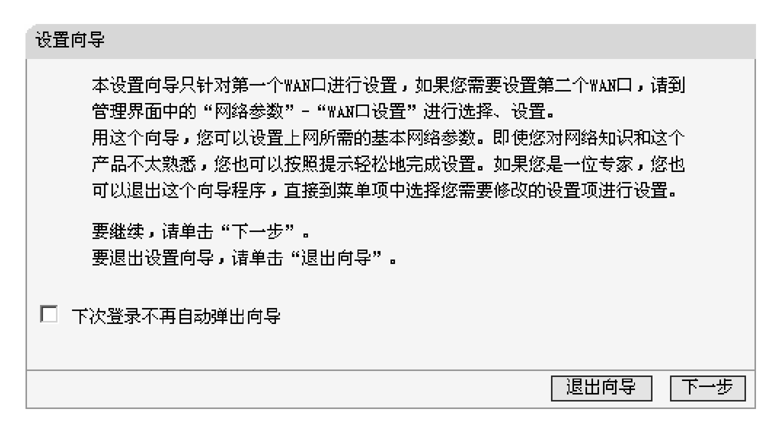
激活浏览器，取消“使用代理服务器”选项或者将路由器的IP地址添加到“代理服务器设置”中的“例外”栏中（在IE中选择“工具－Internet选项－连接－局域网设

置”，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的IP地址，例如http://192.168.1.1。

连接建立起来后，您将会看到下图所示登录界面。您需要以系统管理员的身份登录，即在该登录界面输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。



如果名称和密码正确，浏览器将显示管理员模式的画面，并会弹出一个设置向导的画面（如果没有自动弹出的话，可以单击管理员模式画面左边“设置向导”菜单将它激活）。



单击“下一步”，进入上网方式选择画面。

设置向导

本路由器支持三种常用的上网方式，请您根据自身情况进行选择。

- ○ ADSL虚拟拨号（PPPoE）
- ◉ 以太网宽带 ，自动从网络服务商获取IP地址（动态IP）
- ○ 以太网宽带 ，网络服务商提供的固定IP地址（静态IP）

[上一步] [下一步]

以上画面显示了最常用的三种上网方式，您可以根据自身情况进行选择，然后单 击“下一步”填写上网所需的基本网络参数。

1) 如果您的上网方式为 PPPoE，即 ADSL 虚拟拨号方式，则您需要填写以下内容：

设置向导

您申请ADSL虚拟拨号服务时，网络服务商将提供给您上网帐号及口令，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。

上网账号： username

上网口令： ●●●●●●●●●

[上一步] [下一步]

- **上网帐号**：填入ISP为您指定的ADSL上网帐号，不清楚可以向ISP询问。
- **上网口令**：填入ISP为您指定的ADSL上网口令，不清楚可以向ISP询问。

2) 如果您的上网方式为动态 IP，即您可以自动从网络服务商获取 IP 地址，则您不需要填写任何内容即可直接上网。

3) 如果您的上网方式为静态 IP，即您拥有网络服务商提供的固定 IP 地址，则您需要填写以下内容：

设置向导-静态IP

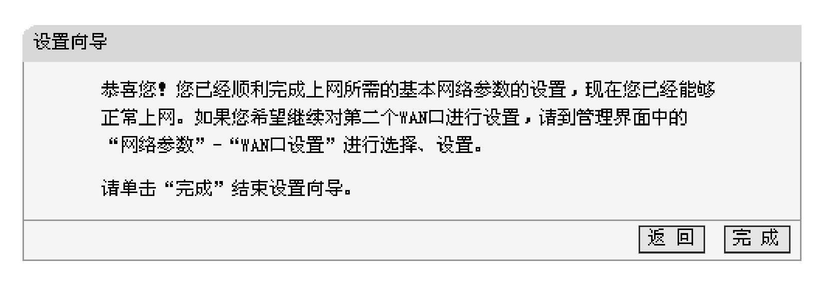
您申请以太网宽带服务，并具有固定IP地址时，网络服务商将提供给您一些基本的网络参数，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。

IP地址：	222.88.88.222	
子网掩码：	255.255.255.0	
网关：	0.0.0.0	（可选）
DNS服务器：	0.0.0.0	（可选）
备用DNS服务器：	0.0.0.0	（可选）

帮 助　　上一步　下一步

- **IP地址**：本路由器对广域网的IP地址，即ISP提供给您的IP地址，不清楚可以向ISP询问。
- **子网掩码**：本路由器对广域网的子网掩码，即ISP提供给您的子网掩码，一般为255.255.255.0。
- **网关**：填入ISP提供给您的网关，不清楚可以向ISP询问。
- **DNS服务器**：填入ISP提供给您的DNS服务器地址，不清楚可以向ISP询问。
- **备用DNS服务器**：可选项，如果ISP提供给您了两个DNS服务器地址，则您可以把另一个DNS服务器地址的IP地址填于此处。

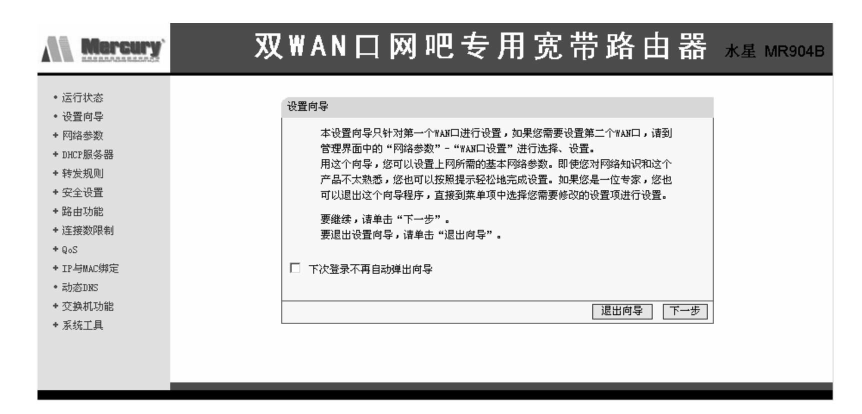
在填写完上网所需的基本网络参数之后，会出现设置向导完成界面。



第5章 配 置 指 南

5.1 启动和登录

在启动和登录成功以后，浏览器会显示管理员模式下的路由器配置页面。



在左侧菜单栏中，共有“运行状态”、“设置向导”、“网络参数”、“DHCP服务器”、“转发规则”、“安全设置”、“路由功能”、“连接数限制”、“QoS”、“IP与MAC绑定”、“动态DNS”、“交换机功能”和“系统工具”十三个菜单。单击某个菜单项，您即可进行相应的功能设置。

在使用过程中，如果您对本产品的功能有任何疑问，您只需单击该页面的“帮助”按钮，即可获得详细的联机帮助。

下面将详细讲解各个菜单的功能。

5.2 运行状态

版本信息

当前软件版本： 3.3.1 Build 070809 Rel.54595n
当前硬件版本： MR904BV1 00000000

LAN口状态

MAC 地址： 00-0A-EB-E6-B8-E4
IP地址： 192.168.1.1
子网掩码： 255.255.255.0

WAN口状态

WAN口：1 线路正常

MAC 地址： 00-0A-EB-E6-B8-E5
IP地址： 222.88.88.222 静态IP
子网掩码： 255.255.255.0
网关： 0.0.0.0
DNS 服务器： 0.0.0.0 , 0.0.0.0

WAN口：2 网线没有插好

MAC 地址： 00-0A-EB-E6-B8-E6
IP地址： 10.20.1.30 动态IP
子网掩码： 255.255.255.0
网关： 0.0.0.0 [释 放]
DNS 服务器： 10.20.1.21 , 0.0.0.0

WAN口流量统计

	当前速率(Kbps)	接收字节数	发送字节数	接收数据包数	发送数据包数
总数据	0	0	0	0	0
WAN口 1	0	0	0	0	0
WAN口 2	0	0	0	0	0

运行时间： 0 day(s) 01:07:25 [刷 新]

本页显示路由器的工作状态。

1) 版本信息

此处显示当前的软、硬件版本。

2) LAN口状态

此处显示当前LAN口的MAC地址、IP地址和子网掩码。

3) WAN口状态

此处显示WAN口（WAN1和WAN2）的MAC地址、IP地址、子网掩码、网关和DNS服务器。同时IP地址右侧将显示用户上网方式（PPPoE/动态IP/静态IP）。如果用户的上网方式为PPPoE（ADSL拨号上网）的话，当用户已经连接上Internet时，此处将会显示用户的上网时间和“断线”按钮，单击此按钮可以进行即时的断线操作，当用户未连接Internet时，此处将会显示“连接”按钮，单击此按钮可以进行即时的连接操作。

4) WAN口流量统计

此处显示WAN口接收和发送的数据流量信息。

5.3 设置向导

请参考第4章的快速安装指南。

5.4 网络参数

- 网络参数
  - LAN口设置
  - WAN口设置
  - WAN口在线检测
  - MAC地址克隆
  - 流量均衡控制
  - ISP均衡控制
  - 均衡策略
  - WAN端口参数

在“网络参数”菜单下面，共有“LAN口设置”、“WAN口设置”、“WAN口在线检测”、“MAC地址克隆”、“流量均衡控制”、“ISP均衡控制”、“均衡策略”和“WAN端口参数”共八个子项。单击其中某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.4.1 LAN口设置

请您选择网络参数下的LAN口设置项，您将进入LAN口的设置界面，如下图示。您可按照下面各子项说明设置该LAN口的参数。

LAN口设置

本页设置LAN口的基本网络参数。

MAC地址： 00-0A-EB-E6-B8-E4

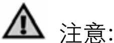
IP地址： 192.168.1.1

子网掩码： 255.255.255.0

注意：当LAN口IP参数（包括IP地址、子网掩码）发生变更时，为确保DHCP server能够正常工作，应保证DHCP server中设置的地址池、静态地址与新的LAN口IP是处于同一网段的，并请重启路由器。

保 存 帮 助

- **MAC地址**：显示路由器对局域网的MAC地址，此值不用设置，也不可更改。
- **IP地址**：请输入本路由器对局域网的IP地址。该IP地址出厂默认值为192.168.1.1，您可以根据您的实际需要设置该值。
- **子网掩码**：请您输入本路由器对局域网的子网掩码，一般为255.255.255.0，局域网中所有计算机的子网掩码必须与此处设置相同。


注意:

1 如果您改变了此处LAN口的IP地址，则您必须用新的IP地址才能登录路由器管理界面，并且局域网中所有计算机的默认网关也必须设置为该IP地址，这样才能正常上网。

2 局域网中所有计算机的子网掩码必须与此处子网掩码相同。

5.4.2 WAN 口设置

请您选择网络参数下的WAN口设置项，您将进入WAN口的设置界面（默认为动态IP设置界面），如下图示。首先请您选择需要设置的WAN口号，通过下拉列表框可选择WAN口1或WAN口2。然后请您选择WAN口的连接类型，即您的上网方式。最后您将进入相应的设置界面，下面将根据您的选择分别介绍这些不同连接类型的WAN口设置。

1) 如果您选择的 WAN 口连接类型是“动态 IP”，即您可以从网络服务商（ISP）自动获取 IP 地址时，其设置界面如下图示。您可以按照下面各子项说明，设置相应的参数。

WAN口设置

WAN口：WAN口1

WAN口连接类型：动态IP

☑ 内部网络，网段为 222.88.88.2-222.88.88.200

更 新　释 放　正在获取网络参数...

IP地址：0.0.0.0

子网掩码：0.0.0.0

网关：0.0.0.0

数据包MTU(字节)：1500 (默认是1500,如非必要，请勿修改.)

☑ 手动设置DNS服务器

DNS服务器：202.96.128.68

备用DNS服务器：202.96.134.133 (可选)

☐ 单播方式获取IP (一般情况下请勿选择.)

请在以下的输入框中输入ISP指定的线路带宽值，如不清楚可以向您的ISP咨询。

下行带宽：100000 Kbps

上行带宽：100000 Kbps

保 存　帮 助

- **WAN口**：该项用来选择您需要设置的WAN口，本路由器对广域网提供两个WAN口，即WAN口1和WAN口2。您可以根据需要选择适当的WAN口进行设置。
- **内部网络**：当WAN口连接的是局域网时，您可以选择该复选框，在右边方框内输入该局域网中的一段网段地址，该WAN口将只转发发往该网段地址的数据包。该项为可选项。
- **连接类型**：上图选择的是“动态IP”上网方式。本路由器支持三种常用的上网方式：动态IP、静态IP、PPPoE方式，您可根据自身情况选择。
- **IP地址**：显示您从ISP的DHCP服务器动态得到的IP地址，它是路由器对广域网的地址。
- **子网掩码**：显示您从ISP的DHCP服务器动态得到的子网掩码。
- **网关**：显示您从ISP的DHCP服务器动态得到的网关。
- **数据包MTU**：请您输入需要限制的数据包的最大长度（MTU），可以输入的范围是576 ～ 1500，默认值为1500。若非必要，请您不要修改该默认值。
- **手动设置DNS服务器**：选择该复选框，您将可以手动设置自己想要的DNS服务器地址。

- **DNS服务器**：显示您从ISP的DHCP服务器动态得到的DNS服务器地址，您也可以在此处手动设置想要的DNS服务器地址。
- **备用DNS服务器**：显示您从ISP的DHCP服务器动态得到的备用DNS服务器地址，您也可以在此手动设置想要的备用DNS服务器地址，也可以不选。

➢ **单播方式获取IP**：如果您的ISP服务器支持以单播方式获取IP地址，请您选择该复选框，您将以单播的方式从ISP获取IP地址。

 注意：

单播方式获取IP是指主机以点对点的单播包向指定的DHCP服务器请求分配IP地址。大多数网络服务商的DHCP服务器支持广播的请求方式，只有少数是支持单播的请求方式。如果您在网络连接正常的情况下无法获取IP地址，可以选择单播的方式（一般情况下不要选择此项）。

➢ **下行带宽**：请您输入该指定WAN口的最大下行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。

➢ **上行带宽**：请您输入该指定WAN口的最大上行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。

➢ **按钮功能**：包括"更新"和"释放"按钮。

- **更新**：单击此按钮，您可以从ISP的DHCP服务器更新WAN口的IP地址、子网掩码、网关、DNS服务器等设置。
- **释放**：单击此按钮，本路由器将发送DHCP释放操作到ISP的DHCP服务器，释放IP设置。

设置完上面的参数后，点击保存按钮，设置的参数将生效。

2) 如果您选择的 WAN 口连接类型是"静态 IP"，即您拥有网络服务商（ISP）提供的固定 IP 地址，其设置界面如下图示。您可以按照下面各子项说明设置相应的参数。

WAN口设置

WAN口： WAN口1

WAN口连接类型： 静态IP

☑ 内部网络，网段为 222.88.88.2-222.88.88.200

IP 地址： 222.88.88.222

子网掩码： 255.255.255.0

网关： 0.0.0.0 (可选)

数据包MTU(字节)： 1500 (默认是1500，如非必要，请勿修改)

DNS服务器： 0.0.0.0 (可选)

备用DNS服务器： 0.0.0.0 (可选)

请在以下的输入框中输入ISP指定的线路带宽值，如不清楚可以向您的ISP咨询。

下行带宽： 100000 Kbps

上行带宽： 100000 Kbps

保 存 帮 助

- **内部网络**：当WAN口连接的是局域网时，您可以选择该复选框，在右边方框内输入该局域网中的一段网段地址，该WAN口将只转发发往该网段地址的数据包。该项为可选项。
- **IP地址**：请您输入ISP提供给您的固定IP地址，它是路由器对广域网的IP地址，不清楚可以向ISP询问。
- **子网掩码**：请您输入ISP提供给您的子网掩码，它是路由器对广域网的子网掩码，一般为255.255.255.0。
- **网关**：请您输入ISP提供给您的网关，不清楚可以向ISP询问。
- **数据包MTU**：请您输入需要限制的数据包的最大长度（MTU），可以输入的范围是576 ～ 1500，默认值为1500。若非必要，请您不要修改该默认值。
- **DNS服务器**：请您输入ISP提供给您的一个DNS服务器地址，不清楚可以向ISP询问，也可以不填。
- **备用DNS服务器**：请您输入ISP提供给您的另一个DNS服务器地址，也可以不填。
- **下行带宽**：请您输入该指定WAN口的最大下行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。
- **上行带宽**：请您输入该指定WAN口的最大上行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。

3) 如果您选择的 WAN 口连接类型是“PPPoE”，即您可以从网络服务商（ISP）自动获取 IP 地址，其设置界面如下图示。您可以按照下面各子项说明设置相应的参数。

WAN口设置

WAN口： WAN口1

WAN口连接类型： PPPoE

上网帐号： username

上网口令： ●●●●●●●●●●●●●●

根据您的需要，请选择对应的连接模式：

◉ 按需连接，在有访问数据时自动进行连接

自动断线等待时间：15 分 (0 表示不自动断线)

○ 自动连接，在开机和断线后自动连接

○ 定时连接，在指定的时间段自动连接

注意：只有当您到“系统工具”菜单的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。

连接时段：从 0 时 0 分到 23 时 59 分

○ 手动连接，由用户手动连接

自动断线等待时间：15 分 (0 表示不自动断线)

连 接　断 线

请在以下的输入框中输入ISP指定的线路带宽值，如不清楚可以向您的ISP咨询。

下行带宽： 8000 Kbps

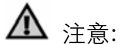
上行带宽： 2000 Kbps

高级设置

保 存　帮 助

- **上网帐号**：请您输入ISP为您指定的ADSL上网帐号，不清楚可以向ISP询问。
- **上网口令**：请您输入ISP为您指定的ADSL上网口令，不清楚可以向ISP询问。
- **按需连接**：选中该复选框，则表示您将采用按需连接模式，即当有局域网的网络访问请求时，系统将自动连接网络。
  - **自动断线等待时间**：若您选择上面的按需连接模式，则您还需在此输入自动断线等待时间（T）。如果T不等于0，则在检测到连续T分钟内，若没有网络访问流量系统则会自动断开网络连接，节省您的上网资源。若T等于0，则表示系统不会自动断线。
- **自动连接**：选中该复选框，则表示您将采用自动连接模式，即在您开机后系统会自动进行连接操作。在使用过程中，如果由于外部原因，网络被断开，则系统会每隔一段时间（30秒）尝试进行连接，直到连接成功为止。

- **定时连接**：选中该复选框，则表示您将采用定时连接模式，即系统在“连接时段”指定的起始时间进行连接操作，在指定的终止时间自动进行断线操作。
  - **连接时段**：若您选择上面的定时连接，则您还需在此设置连接时段，即定时连接的起始和终止时间。
- **手动连接**：选中该复选框，则表示您将采用手动连接模式，即您在需要连接网络时，自己手动进行ADSL拨号连接。与此同时，您还需在此输入自动断线等待时间（T）。具体设置同上面所述。
- **按钮功能**：包括“连接”和“断线”两个按钮。
  - **连接**：单击此按钮，进行即时的连接操作。
  - **断线**：单击此按钮，进行即时的断开操作。
- **下行带宽**：请您输入该指定WAN口的最大下行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。
- **上行带宽**：请您输入该指定WAN口的最大上行带宽(1 ～ 100000 Kbps)。若不清楚，可以向您的ISP咨询。



注意：

1　只有当您在“系统工具”的“时间设置”项，设置了当前时间后，“定时连接”功能才能生效。

2　您可以根据需要选择上面4种连接方式中的任意一种，设置完后可以点击保存按钮，使设置生效。

3　您还可以根据实际需要，进入到“高级设置”界面对相关设置项进行设置、调整。其设置界面如下图示，您可以按照下面各子项说明设置相应的参数。

PPPoE高级设置

数据包MTU(字节)： 1492 (默认是1492，如非必要，请勿修改)
服务名： (如非必要，请勿填写)
服务器名： (如非必要，请勿填写)
☐ 使用ISP指定的IP地址
ISP指定的IP地址： 0.0.0.0
在线检测间隔时间： 0 秒 (0 ～ 120 秒，0 表示不发送)
☐ 手动设置DNS服务器
DNS服务器： 0.0.0.0
备用DNS服务器： 0.0.0.0 (可选)
返 回

保 存　帮 助

- **数据包MTU**: 请您输入需要限制的数据包的最大长度（MTU），默认值为1492。若非必要，请您不要修改该默认值。
- **服务名**：Service Name，若不是ISP特别要求，请不要填写。
- **服务器名**：AC Name，如果不是ISP特别要求，请不要填写。
- **使用ISP指定的IP地址**：选中复选框，您可以设置ISP提供给您的指定IP地址。
  - **ISP指定的IP地址**：请输入您的ISP提供的指定IP地址。
- **在线检测时间间隔**：请您根据需要填写所需的在线检测时间间隔。路由器将根据该时间间隔发送检测信号，以检测服务器是否在线。若该值为0，则表示不发送检测信号。如果您在系统日志中经常发现有“接收PADT,服务端请求断开本次连接”这样的日志信息时，请将该值设为0。

DNS服务器的设置同前面“动态IP”所述，设置完成后可以点击保存按钮，使设置生效。

5.4.3 WAN 口在线检测

选择网络参数下的WAN口在线检测项，可以进入下面设置页面，路由器可以通过该页面，准确地检测线路是否正常，从而达到稳定工作的目的。

WAN口在线检测

本页设置WAN口的在线检测方式。路由器可以通过以下设置准确地检测线路是否正常，从而达到稳定地工作的目的。
请注意：您必须确保所设置的DNS server、被Ping的主机是能够对以下请求做出正确应答的，否则可能会导致路由器工作异常。

WAN1: 线路正常
☐ Ping 检测
Ping目标IP： 0.0.0.0
☐ DNS 请求检测
DNS 服务器IP ： 0.0.0.0

WAN2: 网线没有插好
☐ Ping 检测
Ping目标IP： 0.0.0.0
☐ DNS 请求检测
DNS 服务器IP ： 0.0.0.0

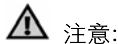
保 存 帮 助

- **Ping检测**：选择此复选框，则您将可以通过PING检测该WAN口是否处于在线的状态。（即：路由器根据自身是否能够ping通指定IP主机来判断是否处于在线状态）。

- **Ping目标IP**：请在该输入框内输入您想Ping的目标主机IP，该IP必须是WAN口所在网络中确实存在的主机IP地址，例如：222.88.88.5。

➢ **DNS请求检测:** 选择此复选框，则您将可以通过DNS查询来检测该WAN口是否处于在线的状态。（即：路由器根据自身是否能够收到相应的DNS应答来判断是否处于在线状态）。

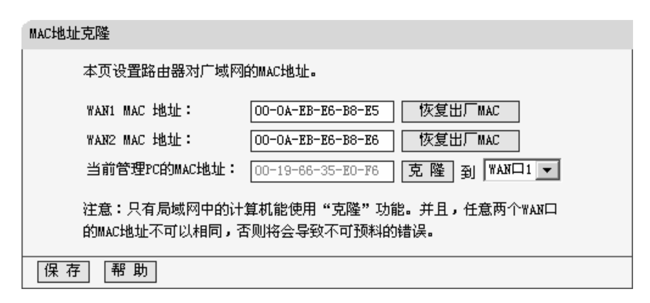
- **DNS服务器IP:** 请在该输入框内输入WAN口所在网络中确实存在的DNS服务器的IP地址，例如：202.96.134.133。


注意:

您必须确保所设置的DNS 服务器、被Ping的主机是能够对以上请求做出正确应答的，否则可能会导致路由器工作异常。

5.4.4 MAC 地址克隆

选择网络参数下的MAC地址克隆项，您将进入下面的设置界面，如下图示。您可按照下面各子项说明正确使用该功能。



➢ **WAN1 MAC地址**: 显示当前路由器对广域网的MAC地址，此值一般不用更改。但某些 ISP可能要求对MAC地址进行绑定，此时ISP会提供一个有效的MAC地址给用户，您只要根据它所提供的值，输入到“MAC地址”栏，然后单击“保存”，即可根据ISP的要求更改本路由器对广域网的MAC地址。

➢ **WAN2 MAC地址:** 同上面WAN1 MAC地址。

➢ **恢复出厂MAC**: 若您要恢复本路由器对广域网的出厂默认MAC地址，则您可以单击此按钮来恢复。

➢ **当前管理PC的MAC地址**: 显示当前正在进行管理操作的计算机的MAC地址。

➢ **克隆**: 若您想把当前正进行管理操作的PC机的MAC地址填入到对应的WAN口“MAC地址”栏内，请您先选择克隆到的WAN口类型，再点击克隆按钮即可。



注意:

只有局域网中的计算机能使用“克隆MAC地址”功能。

5.4.5 流量均衡控制

选择网络参数下的流量均衡控制，您可以进入下面的设置界面。



- **开启/禁用WAN口**： 该项用来选择是否启用WAN1或WAN2口的流量均衡控制。选择之后，请您点击保存按钮使设置生效。
- **附加IP地址调度规则**: 该项通过启用或禁用按钮来选择是否启用附加IP地址调度规则。
  - **备份**: 您可以点击此按钮，备份现存的列表文件。
  - **载入**: 您可以点击此按钮，将指定的列表文件载入，您可以通过浏览按钮选择指定的文件。
- **已设附加IP地址调度规则列表**: 该项显示用户已设的附加IP地址调度规则。
  - **ID**: 显示条目序号。
  - **指定出口**: 显示该调度规则使用的WAN口类型。设置该项后，LAN中的某一部分IP地址将优先（或只能）从该WAN口连接Internet，或者当访问Internet的某些IP地址时优先（或只能）经过该WAN口。
  - **地址类型**: 显示该调度规则指定的IP地址段类型，即局域网内源IP地址（段）或Internet上的目的IP地址（段）类型。

- **协议:** 显示网络连接时采用的协议类型。
- **IP地址（段）**显示该调度规则指定的局域网内的源IP地址段或Internet上的目的IP地址（段）。
- **端口（段）:** 显示该调度规则针对的端口范围。
- **启用:** 您可以通过该项来确定是否启用该调度规则，选中该复选框表示启用，否则表示禁用。
- **配置:** 显示对调度规则的超级链接——编辑或删除。

➢ **移动:** 您可以通过该项来改变原来的规则排列顺序。例如，将第3条调度规则改为第2条调度规则，操作如上图界面所示，填完后点击移动按钮即可实现。

➢ **添加新条目:** 点击该按钮，您可以增加新的调度规则条目，详见下面所述。

➢ **使所有条目生效:** 点击该按钮，您可以使表中的所有调度规则条目生效。

➢ **使所有条目失效:** 点击该按钮，您可以使表中的所有调度规则条目失效。

➢ **删除所有条目:** 点击该按钮，您可以删除列表中所有已设的或禁用的调度规则条目。

5.4.5.1　　添加或编辑流量均衡控制

点击上页界面中的添加新条目或规则条目右侧的编辑按钮，您将进入下面的设置界面。该页用来设置路由器WAN口的流量分配。用户可以指定局域网中的某些地址的数据包优先从某一个WAN口转发，或者指定发往某些Internet地址的数据包优先从某一个WAN口转发。您可按照下面各子项说明来添加新的调度规则或编辑已有的调度规则。

流量均衡控制

☑ 启用

规则选择：来自LAN口的，源IP/协议/端口(段)为

IP地址(段)：192.168.1.23 - 192.168.1.254

端口(段)：1024 - 8080

协 议：TCP

数据包通过策略：优先

转发路径：WAN口1

保 存　返 回　帮 助

➢ **启用:** 请您选择是否启用该调度规则。

- **规则选择:** 该项提供两种调度规则，一种是"来自LAN口的，源IP/协议/端口(段)为"，该选项主要用来指定局域内中的某些地址的数据包，优先从某一个WAN口转发出去。另一种是"发往WAN口的，目的IP/协议/端口（段）为"，该选项主要用来指定发往某些Internet地址的数据包，优先从某一个WAN口转发出去，您可以根据需要选择。
- **IP地址段:** 请您输入该调度规则采用的局域网内的源IP地址段或Internet上的目的IP地址（段）。IP地址（段）的输入格式为：222.88.88.254（或者192.168.1.23-192.168.1.254）。
- **端口（段）:** 请您输入该调度规则针对的端口范围。
- **协议:** 请您输入连接采用的协议类型，如TCP或UDP等。
- **数据包通过策略:** 请您选择数据包通过该规则时采用的策略类型，优先或只能。"优先"表示数据包优先从指定的WAN口进行转发，"只能"表示数据包只能从指定的WAN口转发出。
- **转发路径:** 请您选择数据包转发时采用的WAN口类型（WAN1或WAN2口）。

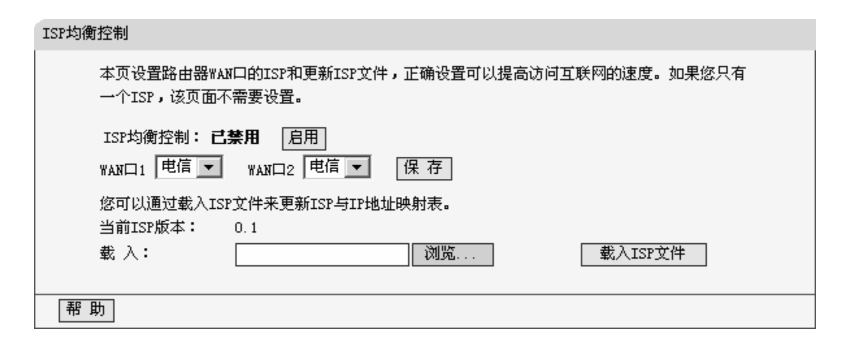

注意:

1 只有当"附加IP地址调度规则"启用时，列表中的各条规则才有效。

2 列表中的各条目遵循优先匹配的原则，即按照已设附加IP地址调度规则表中的条目顺序，从上到下选择适当的规则来匹配。

5.4.6 ISP 均衡控制

选择网络参数下的ISP均衡控制项，您将进入下面的设置界面。该页主要设置路由器WAN口的ISP类型并更新ISP文件，正确设置该项可以对不同ISP的所有数据包进行自动分流，从而提高互联网的访问速度。如果您只有一个ISP，则该页面不需要设置。下面您可按照各子项说明正确使用该功能。



- **ISP均衡控制:**选择是否启用ISP均衡控制。只有启用后，该项的设置才能生效。

➢ **WAN口1/WAN口2:**请您分别为两个WAN口选择对应的ISP类型（电信或网通）。设置该项后，路由器可根据待转发数据包的目的地址，快速地确定WAN出口，从而提高网络访问速度。

➢ **载入:**您可以通过该项载入最新的ISP文件，以此来更新ISP与IP地址映射表。

5.4.7 均衡策略

选择网络参数下的ISP均衡控制项，您将进入下面的设置界面。该页用来设置路由器多WAN口的数据包转发策略，这些策略主要依据3种原则，速度优先、IP地址对优先、应用程序优先。可以通过4个数据表来查询，它们分别是速度检测表、快速连接表、IP地址对表、应用程序表。您可按照下面各子项说明来设置相应的参数。

均衡策略

本页设置路由器WAN口的转发策略，这些策略主要依据3种原则，速度优先、IP地址对优先、应用程序优先。为此我们采用了4个数据表用于查询，它们分别是速度检测表、快速连接表、IP地址对表、应用程序表，以下与时间相关的参数就是针对这些表进行设置的。由于这些缺省值都是经过测试的，如果您不是很确定的话，请不要进行修改。

多WAN口的WAN选择规则：

☑ 速度优先

速度检测列表快速老化时间： 2 秒（1 ~ 5），缺省 2

速度检测列表老化时间： 5 秒（2 ~ 10），缺省 5

快速连接阀值： 100 毫秒（20 ~ 200），缺省 100

速度优先列表老化时间： 120 秒（1 ~ 300），缺省 120

速度优先列表强制老化时间： 600 秒（10 ~ 1200），缺省 600

☑ IP地址对优先

IP地址对优先列表老化时间： 360 秒（1 ~ 1200），缺省 360

IP地址对优先列表强制老化时间： 600 秒（10 ~ 2400），缺省 600

☑ 应用程序优先

应用程序优先列表老化时间： 600 秒（1 ~ 1800），缺省 600

应用程序优先列表强制老化时间： 1200 秒（10 ~ 3600），缺省 1200

保 存　帮 助

➢ **速度优先:**若您选择该项，则当尝试建立新连接时，如果某一个WAN口表现得比其它WAN口快，那么数据就会从这个WAN口转发。

- **速度检测列表快速老化时间:**在该时间间隔内（缺省为2秒），如果某一个条目从来没有被使用过，该条目就会被删除。

- **速度检测列表老化时间 :**在该时间间隔内（缺省为5秒），无论该条目是否曾经被使用过，该条目都会被删除。
- **快速连接阈值:**在该时间间隔内（缺省为100毫秒），如果收到了来自Internet的应答，那么这个连接就会被认为是一个“快速”的连接。
- **速度优先列表老化时间:**在该时间间隔内（缺省为120秒），如果某一个条目从来没有被使用过，该条目就会被删除。
- **速度优先列表强制老化时间:**在该时间间隔内（缺省为600秒），无论一个条目是否曾经被使用过，该条目都会被删除。

➢ **IP地址对优先:**如果LAN中的主机A与Internet中的主机B曾经建立过连接，那么这两个主机间的后续的连接都会按照原有的WAN口进行转发。

- **IP地址对优先列表老化时间:**在该时间间隔内（缺省为360秒），如果某一个条目从没有被使用过，该条目就会被删除。
- **IP地址对优先列表强制老化时间:在该时间间隔内（缺省为600秒），无论一个条目是否曾经被使用过，该条目都会被删除。**

➢ **应用程序优先:**如果某台主机上的一个应用程序发起了超过2个以上的连接，那么所有基于这个应用的连接都会选择同一个WAN口进行转发。

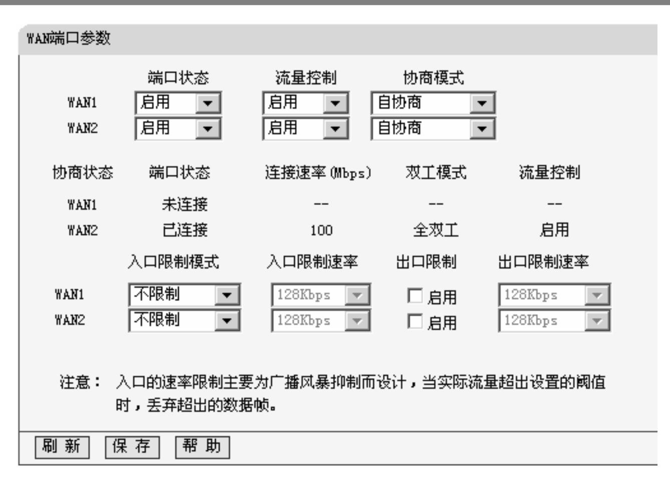
- **应用程序优先列表老化时间:**在该时间间隔内（缺省为600秒），如果某一个条目从没有被使用过，该条目就会被删除。
- **应用程序优先列表强制老化时间:**在该时间间隔内（缺省为1200秒），无论一个条目是否曾经被使用过，该条目都会被删除。


注意:

以上的时间间隔缺省值都是经过测试的，如果您对该值不是很确定的话，请您不要随意修改。

5.4.8 WAN 端口参数

选择网络参数下的WAN端口参数，您将进入下面的设置界面。该页面提供端口状态、端口流量控制等设置。您可以按照下面各子项说明正确设置这些参数。



- **端口状态表**：该项用来设置并显示WAN端口的状态信息。
  - **端口状态**：您可以根据需要设置WAN口的状态，启用或禁用。
  - **流量控制**：您可以根据需要启用或禁用流控模式。启用表示对该端口的数据流量进行控制，反之则不加控制。
  - **协商模式**：您可以根据需要选择协商模式：自协商、10M半双工、10M全双工、100M半双工或100M全双工模式。
- **协商状态表**：该项用来显示端口的协商状态信息。
  - **端口状态**：显示端口连接状态，即是否已经连接上。
  - **连接速率**：显示端口连接采用的速率。
  - **双工模式**：显示端口通信采用的双工模式，全双工或半双工。
  - **流量控制**：显示端口是否启用了流量控制。
- **端口限制信息表**：该项用来设置并显示端口的各种限制信息。
  - **入口限制模式**：该项用来选择对进入该WAN口的数据包采用的限制类型：所有帧、FLOOD、广播和多播、广播或不限制。
  - **入口限制速率**：该项用来限制进入该WAN口的数据包速率，其中可选项有128Kbps、256Kbps、512Kbps、1Mbps、2 Mbps、4 Mbps、8Mbps。
  - **出口限制**：选中该复选框表示启用出口限制，即对该WAN口转发的数据包进行限制，不选中该复选框则表示不启用出口限制。
  - **出口限制速率**：该项用来限制从该WAN口转发的数据包速率，其中可选项有128Kbps、256Kbps、512Kbps、1Mbps、2Mbps、4Mbps、8Mbps。

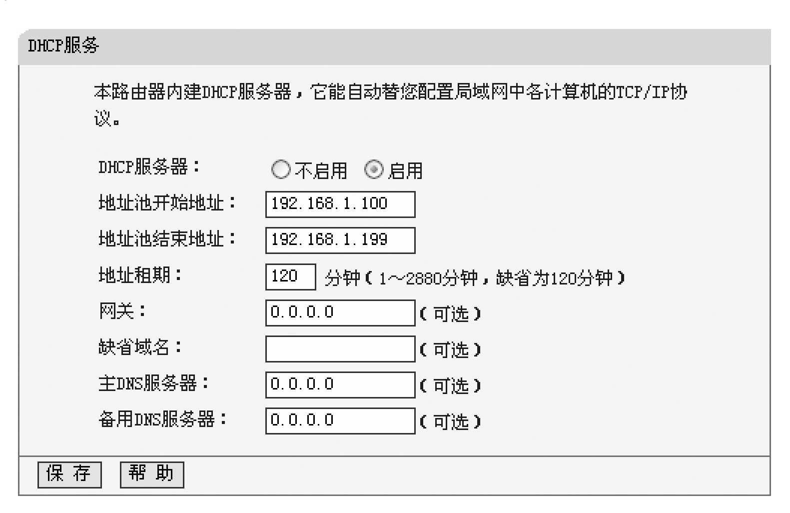
5.5 DHCP 服务器

- DHCP服务器
  - DHCP服务
  - 客户端列表
  - 静态地址分配

DHCP服务器主要用来自动配置和管理网络内部主机的TCP/IP参数。在“DHCP服务器”菜单下面，有“DHCP服务”、“客户端列表”和“静态地址分配”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

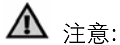
5.5.1 DHCP 服务

选择DHCP服务器下的DHCP服务，您将进入下面的设置界面。对用户来说，为局域机配置TCP/IP协议参数并不是一件容易的事，它包括IP地址、子网掩码、网关、以及DNS服务器的设置等。幸运的是，DHCP服务器提供了这种功能。如果您使用本路由器的DHCP服务器功能的话，您可以让DHCP服务器自动替您配置局域网中各计算机的TCP/IP协议。您可按照下面各子项说明正确设置这些参数。



- **DHCP服务器**：若您想使用DHCP的自动配置TCP/IP参数功能，请您选择启用。
- **地址池开始地址**：请您输入DHCP服务器自动分配IP地址的起始地址。
- **地址池结束地址**：请您输入DHCP服务器自动分配IP地址的结束地址。

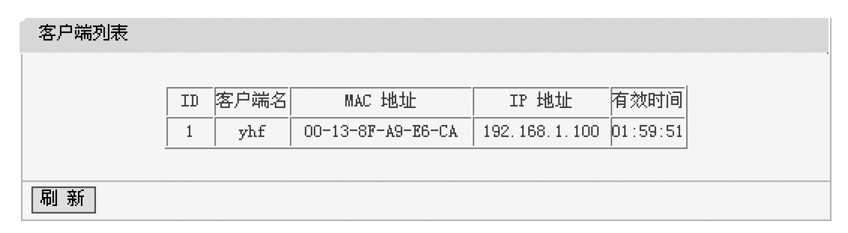
- **地址租期**：请您输入所分配IP地址的有效使用时间，超时将重新分配。
- **网关**：请您输入路由器LAN口的IP地址，本路由器缺省是192.168.1.1。
- **缺省域名**：请您输入本地网域名，也可以不填。
- **主DNS服务器**：请您输入ISP提供的DNS服务器地址，不清楚可以向ISP询问，也可以不填。
- **备用DNS服务器**：如果ISP给您提供了两个DNS服务器地址，则请您输入另一个DNS服务器的IP地址，也可以不填。


注意:

为了使用本路由器的DHCP服务器功能，局域网中计算机的TCP/IP协议必须设置为"自动获得IP地址"，并且使用路由器的该功能时，必须先重启路由器后才能生效。

5.5.2 客户端列表

选择DHCP服务器下的客户端列表，您将进入下面界面。该客户端列表罗列了所有通过DHCP获得IP的主机信息，具体如下图示：


客户端列表

ID	客户端名	MAC 地址	IP 地址	有效时间
1	yhf	00-13-8F-A9-E6-CA	192.168.1.100	01:59:51

刷 新

- **ID**：条目序号。
- **客户端名**：显示分配到IP地址的客户端的计算机名。
- **客户端MAC**：显示分配到IP地址的客户端的计算机的MAC地址。
- **已分配IP地址**：显示DHCP服务器分配给客户端的计算机的IP地址。
- **有效时间**：显示主机通过DHCP获得IP地址后，该IP地址剩余的有效时间。客户端软件会在租期到期前自动续约。

5.5.2.1 静态地址分配

选择DHCP服务器下的静态地址分配，您将进入下面的设置界面。为了方便您对局域网中计算机的IP地址进行控制，本路由器内置了静态地址分配功能。它

可以为指定MAC地址的计算机预留静态IP地址。之后，若此计算机请求DHCP服务器分配IP地址时，DHCP服务器将自动给它分配此预留的IP地址。具体设置见下图示:



- **静态地址条目表**: 显示静态地址条目信息。
  - **MAC地址**: 显示预留了IP地址的计算机的MAC地址。
  - **IP地址**: 显示预留的IP地址。
  - **状态**: 显示该条目是否生效。
  - **配置**: 显示对该条目进行的超级链接——编辑或删除。
- **添加新条目**: 点击该按钮，您可以增加新的静态地址条目，详见后面所述。
- **使所有条目生效**: 点击该按钮，您可以使所有静态条目生效。
- **使所有条目失效**: 点击该按钮，您可以使所有静态条目失效。
- **删除所有条目**: 点击该按钮，您可以删除当前列表中的所有启用或未启用的静态条目。

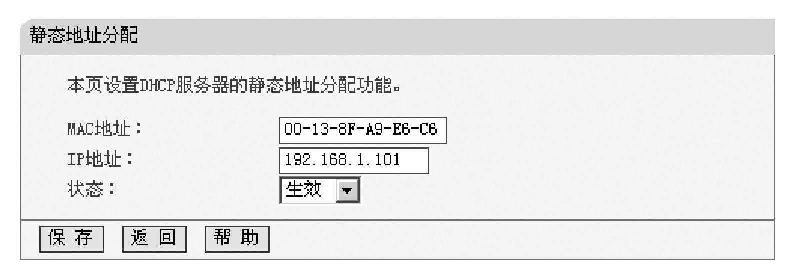


注意:

此功能需要在重启路由器后才能生效。

5.5.2.2 添加或编辑静态地址

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面。该页用来设置静态地址条目。



➢ **MAC地址**：请您输入预留了IP地址的计算机的MAC地址。

➢ **IP地址**：请您输入要预留的IP地址。

➢ **状态**：请您选择该条目是否生效。

设置完以上三项后，点击保存按钮，该设置将会在静态地址条目表中显示。

5.6 转发规则

- 转发规则
  - 虚拟服务器
  - 特殊应用程序
  - DMZ主机
  - UPnP设置

在“转发规则”菜单下面，有“虚拟服务器”、“特殊应用程序”、“DMZ主机”和“UPnP设置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 虚拟服务器

选择转发规则下的虚拟服务器，您将进入下面的设置界面。本路由器自身集成了防火墙功能，在路由器默认设置下，广域网中的计算机不能通过本路由器访问局域网中的某些服务器。但是，为了让路由器既保护局域网内部不被侵袭，又方便广域网中合法的用户访问，路由器提供了虚拟服务器功能。虚拟服务器可以定义一个服务端口，外网所有对此端口的服务请求都将被重新定位给路由器指定的局域网中的服务器，这样外网的用户便能成功访问局域网中的服务器，而不影响局域网内部的网络安全。具体设置界面如下图示。

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

ID	服务端口	IP地址	协议	状态	配置
1	80	192.168.1.23	TCP	生效	编辑 删除
2	1024-8080	192.168.1.180	UDP	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

- **虚拟服务器条目表**：显示虚拟服务器条目信息。
  - **服务端口**：显示WAN端服务端口，即路由器提供给广域网的服务端口，外网对该端口的访问都将重定位到局域网中指定的服务器。
  - **IP地址**：显示局域网中指定为服务器的计算机的IP地址。外网对该局域网的访问都将重定位到该指定的计算机。
  - **协议**：显示数据包的协议类型。
  - **状态**：显示条目的状态。只有生效时，该条目的设置才起作用。
  - **配置**：显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以添加新的虚拟服务器条目。
- **使所有条目生效**：点击该按钮，您可以使所有虚拟服务器条目生效。
- **使所有条目失效**：点击该按钮，您可以使所有虚拟服务器条目失效。
- **删除所有条目**：点击该按钮，您可以删除所有已设的虚拟服务器条目。

5.6.1.1 添加或编辑虚拟服务器

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面。下面以添加新的虚拟服务器条目为例。

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号：1024-8080 (XX-XX or XX)

IP地址：192.168.1.180

协议：UDP

状态：生效

常用服务端口号：--请选择--

保 存　返 回　帮 助

- **服务端口号**：请您输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。如上界面所示。
- **常用服务端口号**：请您在该项选择服务端口号。在“常用服务端口”中，列出了常用协议的端口，您可以直接从其中选择一个，系统会直接将选中的端口填入服务端口号中。对于常用服务端口中没有列出的端口，您也可以在服务端口号处手动输入。

设置完成后，请点击保存按钮，然后在您的局域网的服务器上进行相应的设置，这样，广域网中的计算机便可以成功访问局域网中的服务器了。

举例：

如果在局域网中添加您的HTTP服务器，端口号为80，IP地址为192.168.1.23；其它服务器，端口号为1024-8080，地址为 192.168.1.180（该条目设置，请见上面添加新的虚拟服务器界面示意图）。这时您需要指定如下的虚拟服务器映射表。



虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

ID	服务端口	IP地址	协议	状态	配置
1	80	192.168.1.23	TCP	生效	编辑 删除
2	1024-8080	192.168.1.180	UDP	生效	编辑 删除

添加新条目　使所有条目生效　使所有条目失效　删除所有条目

上一页　下一页　帮 助

 注意：

如果设置了服务端口为80的虚拟服务器，则需要将“系统工具”菜单中的“远端WEB管理”项的WEB管理端口设置为80以外的值，如8080。否则会发生冲突，从而导致虚拟服务器设置无效。

5.6.2 特殊应用程序

选择转发规则下的特殊应用程序，您将进入下面的设置界面。某些程序需要多条连接，如Internet网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的NAT路由器下工作。然而，特殊应用程序使得某些这样的应用程序能够在NAT路由器下工作。当一个应用程序给触发端口上发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。


特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

ID	触发端口	触发协议	开放端口	开放协议	状态	配置
1	630	ALL	1020-1030	ALL	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

➢ **虚拟服务器条目表**：显示虚拟服务器条目信息。

- 触发端口 显示应用程序首先发起连接的端口，即触发端口。

 注意：

触发端口是为应用程序申请建立连接时，路由器指定的用于触发应用程序的端口。只有给该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。

- **触发协议**：显示触发端口上使用的协议，选项有ALL、UDP和TCP。
- **开放端口**：显示该特殊应用程序条目采用的开放端口。

 注意：

开放端口是为应用程序提供服务的多个端口。当给触发端口上发起连接后，开放端口打开，之后应用程序便可以给这些开放端口上发起后续的连接。

- **开放协议**：显示开放端口采用的协议，选项有ALL、UDP和TCP。
- **状态**：显示该条目状态，只有状态为生效时，本条目所设的规则才能生效。
- **配置**：显示对该条目的超级链接——编辑或删除。

➢ **添加新条目**：点击该按钮，您可以在列表中添加新的条目，详见下面章节所述。

➢ **使所有条目生效**：点击该按钮，您可以将该列表中的所有条目的状态设为“生效”。

➢ **使所有条目失效**：点击该按钮，您可以将该列表中的所有条目的状态设为“失效”。

- **删除所有条目**：点击该按钮，您可以删除当前已设的所有条目。

5.6.2.1 添加或编辑特殊应用程序

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面。

特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

触发端口： 630
触发协议： ALL
开放端口： 1020-1030
开放协议： ALL
状态： 生效

常用应用程序： --请选择--

保 存　返 回　帮 助

- **触发端口**：请您输入应用程序首先发起连接的端口触发号，如上图示。
- **开放端口**：请您输入为应用程序提供服务的开发端口号，如上图示。可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。
- **常用应用程序**：请您在该项选择应用程序。在“常用应用程序”中，列出了常用的应用程序，您可以直接在其中选中一个，系统会直接将选中的应用程序的触发端口和开发端口号自动填入到对应项中。对于“常用应用程序”中没有列出的端口，您也可以在触发端口和开放端口处手动输入。

5.6.3 DMZ 主机

选择转发规则下的DMZ主机，您将进入下面的设置界面。在某些特殊情况下，我们需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。设置界面如下。

DMZ主机

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。
（注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。）

DMZ 状态：　◉启用　○不启用

DMZ 主机IP地址：　192.168.1.101

保 存　帮 助

➢ **DMZ主机IP地址**：请您输入局域网中指定为DMZ主机的IP地址。

设置步骤：

首先在DMZ主机IP地址栏内输入欲设为DMZ主机的局域网计算机的IP地址，然后选中“启用”，最后单击“保存”按钮，即可完成DMZ主机的设置。


注意：

设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。

5.6.4　UPnP 设置

选择转发规则下的UPnP设置，您将进入下面的设置界面。依靠UPnP（Universal Plug and Play）协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP和Windows ME系统上安装的MSN Messenger，在使用音频和视频通话时就可以利用UPnP协议，这样原本受限于NAT的功能便可以恢复正常使用。



ID	应用描述	外部端口	协议类型	内部端口	IP地址	状态	删除
1	ftp	21	TCP	21	192.168.1.100	√	☐

➢ **UPnP设置列表**：显示UPnP条目信息。

- 应用描述：显示应用程序通过UPnP向路由器请求端口转换时的描述。
- 外部端口：显示端口转换时采用的路由器端口号。

- 协议类型：表明是对TCP还是UDP进行端口转换。
- 内部端口：显示需要进行端口转换的主机端口号。
- IP地址：显示需要进行端口转换的主机IP地址。
- 状态：显示条目状态。“√”表示应用程序请求并启用了端口转换；"×"表示应用程序请求了端口转换，但并没有启用。

使用UPnP的方法如下:

1) 如果您的电脑开启了防火墙功能, 请您在Windows 防火墙界面的例外项中, 选则启用UPnP框架程序。具体操作方法步骤为：开始→控制面板→安全中心→ Windows 防火墙→例外→选中UPnP框架。若例外项中没有UPnP项, 则点击添加程序，再选中UPnP功能即可。

2) 在路由器UPnP界面中点击“启用UPnP”按钮开启UPnP功能。

3) 当MSN Messenger等程序在运行中使用本功能时, 按“刷新”按钮可以看到端口转换信息。端口转换信息由应用程序发出请求时提供。

4) 不使用时请单击“关闭UPnP”按钮，关闭UPnP功能。


注意:

因为现阶段版本的UPnP协议的安全性还未得到充分保证，所以在不需要时请关闭UPnP功能。只有支持UPnP协议的应用程序才能使用本功能，MSN Messenger还需要操作系统的支持（如Windows XP/ME）。

5.7 安全设置

- 安全设置
  - 防火墙设置
  - IP地址过滤
  - 域名过滤
  - MAC地址过滤
  - 攻击防护

在“安全设置”菜单下面, 共有“防火墙设置”、“IP地址过滤”、“域名过滤”、“MAC地址过滤”和“攻击防护”五个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 防火墙设置

选择安全设置下的防火墙设置，您将进入下面的设置界面。本节介绍防火墙的各个过滤功能的开启与关闭设置。只有防火墙的总开关是开启的时候，后续的“IP地址过滤”、“域名过滤”、“MAC地址过滤”才能够生效，反之，则失效。

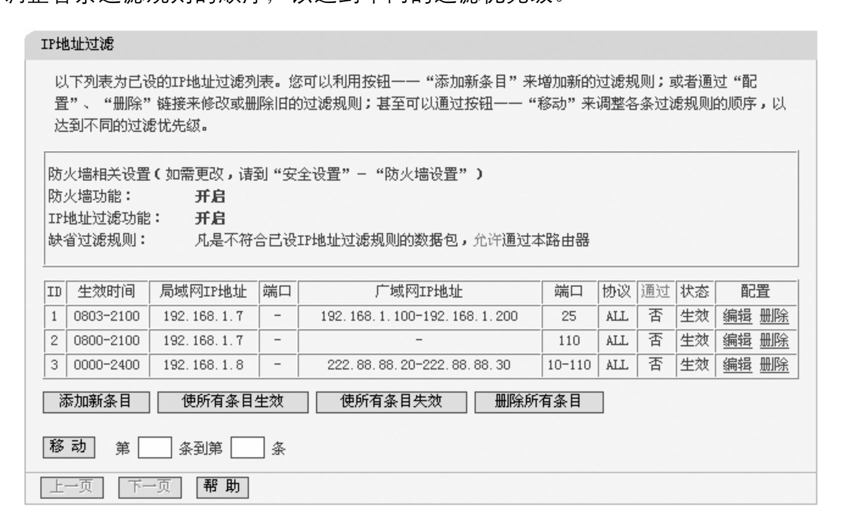


- **开启防火墙**：请您选择是否开启防火墙功能。这是防火墙的总开关，当该开关关闭时，“IP地址过滤”、“域名过滤”、“MAC地址过滤”功能将全部失效。
- **开启IP地址过滤** ：请您选择是否开启防火墙的IP地址过滤功能，只有选择该项时，IP地址过滤设置才能生效。
- **开启域名过滤**：请您选择是否开启防火墙的域名过滤功能，只有选择该项时，域名过滤设置才能生效。
- **开启MAC地址过滤**：请您选择是否开启防火墙的MAC地址过滤功能，只有选择该项时，MAC地址过滤设置才能生效。
- **开启攻击防护**：请您选择是否开启防火墙的攻击防护功能。

5.7.2 IP 地址过滤

选择安全设置下的IP地址过滤，您将进入下面的设置界面。本页显示已设的IP地址过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通

过“编辑”、“删除”链接来修改或删除旧的过滤规则；甚至可以通过按钮—“移动”来调整各条过滤规则的顺序，以达到不同的过滤优先级。


IP地址过滤

以下列表为已设的IP地址过滤列表。您可以利用按钮——“添加新条目”来增加新的过滤规则；或者通过“配置”、“删除”链接来修改或删除旧的过滤规则；甚至可以通过按钮——“移动”来调整各条过滤规则的顺序，以达到不同的过滤优先级。

防火墙相关设置（如需更改，请到“安全设置”－“防火墙设置”）
防火墙功能： 开启
IP地址过滤功能： 开启
缺省过滤规则： 凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0803-2100	192.168.1.7	-	192.168.1.100-192.168.1.200	25	ALL	否	生效	编辑 删除
2	0800-2100	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0000-2400	192.168.1.8	-	222.88.88.20-222.88.88.30	10-110	ALL	否	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

移动 第 条到第 条

上一页 下一页 帮助

- **IP地址过滤条目表**：显示IP地址过滤条目信息。
  - **生效时间**：显示规则生效的起始时间和终止时间。格式为hhmm，例如0803，表示8时3分。
  - **局域网IP地址**：显示局域网中被控制的计算机的IP地址，为空表示对局域网中所有计算机进行控制。这里可以是一个IP地址段，例如192.168.1.100－192.168.1.200。
  - **（局域网）端口**：显示局域网中被控制的计算机的服务端口，为空表示对该计算机所有服务端口进行控制。这也可以是一个端口段，例如1024－8080。
  - **广域网IP地址**：显示广域网中被控制的网站的IP地址，为空表示对整个广域网进行控制。这也可以是一个IP地址段，例如222.88.88.20－222.88.88.222。
  - **（广域网）端口**：显示广域网中被控制的网站的服务端口，为空表示对该网站的所有服务端口进行控制。这也可以是一个端口段，例如：10-110。
  - **协议**：显示被控制的数据包所使用的协议。
  - **通过**：显示符合本条目设置规则的数据包是否可以通过路由器。
  - **状态**：显示本条目状态，即是否使本条过滤规则生效。
  - **配置**：显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以在过滤列表中添加新的过滤条目。详见后面所述。

- **使所有条目生效**: 点击该按钮, 您可以设置表中所有过滤条目的状态为“生效”。
- **使所有条目失效**: 点击该按钮, 您可以设置表中所有过滤条目的状态为“失效”。
- **删除所有条目**: 点击该按钮, 您可以删除当前表中已设的所有过滤条目。
- **移动**: 通过条目序号, 您可以将某条记录移动到另一个位置, 以达到不同的过滤优先级。

5.7.2.1 添加或编辑 IP 地址过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮, 您将进入下面的设置界面。界面中的各参数说明, 请见上面IP地址过滤条目表所述。



若您需要添加新的IP地址过滤条目或修改已存的条目, 只需要正确设置上面各参数, 然后点击保存按钮即可。下面将举例说明。

举例:

设置局域网中IP地址为192.168.1.7的计算机在8:00-21:00时段内不能收发邮件; IP地址为192.168.1.8的计算机全天均不能访问IP为202.96.134.12 的网站, 对局域网中的其它计算机则不做任何限制。

设置步骤:

首先请您在“防火墙设置”中打开防火墙总开关, 然后再开启“IP地址过滤”, 并设置“缺省过滤规则”为“凡是不符合已设IP地址过滤规则的数据包, 允许通过本路由器”。最后, 在添加或编辑界面中按照以上数据要求添加新的过滤条目, 添加设置界面如上图所示。下面为添加后的IP地址过滤条目表。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0800-2100	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0800-2100	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

5.7.3 域名过滤

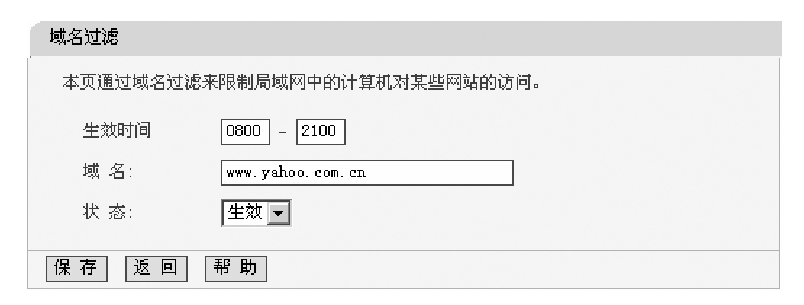
选择安全设置下的域名过滤，您将进入下面的设置界面。本页显示已设的域名过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。



- **域名过滤条目表**：显示域名过滤的条目信息。
  - **生效时间**：显示规则生效的起始时间和终止时间。格式为hhmm，例如0803，表示8时3分。
  - **域名**：显示您希望控制的域名。
  - **状态**：显示本条目状态，即过滤规则是否生效。
  - **配置**：显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以添加新的过滤条目。
- **使所有条目生效**：点击该按钮，您可以将列表中的所有过滤条目的状态设置为“生效”。
- **使所有条目失效**：点击该按钮，您可以将列表中的所有过滤条目的状态设为“失效”。
- **删除所有条目**：点击该按钮，您可以删除该列表中的所有过滤条目。

5.7.3.1 添加或编辑域名过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面，界面中各参数说明见前面域名过滤条目表中所述。



举例:

设置局域网中的计算机在08:00-21:00时段内不能访问“www.yahoo.com.cn”，08:00-24:00时段内不能访问“sina.com”，全天不能访问所有以“.net”结尾的网站，这时您需要设置如下的域名过滤表:

设置步骤:

首先在“防火墙设置”中打开防火墙总开关，然后 开启“域名过滤”，最后，点击添加新按钮，在添加或编辑界面中按照以上数据要求设置新的域名过滤条目，设置界面如上图所示。下面为添加后的IP地址过滤条目表。

ID	生效时间	域 名	状 态	配 置
1	0800-2100	www.yahoo.com.cn	生效	编辑 删除
2	0800-2400	sina.com	生效	编辑 删除
3	0000-2400	.net	生效	编辑 删除

5.7.4 MAC 地址过滤

选择安全设置下的域名过滤，您将进入下面的设置界面。本页显示已设的MAC地址过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。

MAC地址过滤

本页通过MAC地址过滤来控制局域网中计算机对Internet的访问。

防火墙相关设置（如需更改，请到“安全设置”－“防火墙设置”）
防火墙功能： **开启**
MAC地址过滤功能： **开启**
缺省过滤规则： 禁止 列表中已启用的MAC地址访问Internet，允许其他MAC地址访问Internet

ID	MAC地址	描 述	状 态	配 置
1	00-13-8F-A9-E6-CB	张三的计算机	生效	编辑 删除
2	00-13-96-6B-6E-A9	李四的计算机	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

- **MAC地址过滤表**：显示MAC地址过滤条目信息。
  - **MAC地址**：显示您希望控制的计算机的MAC地址。
  - **描述**：显示对该计算机的适当描述。
  - **状态**：显示本条目状态，即本条过滤规则是否生效。
  - **配置**：显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以在过滤列表中添加新的过滤条目。
- **使所有条目生效**：点击该按钮，您可以将该列表中所有过滤条目的状态设为“生效”。
- **使所有条目失效**：点击该按钮，您可以将该列表中所有过滤条目的状态设为“失效”。
- **删除所有条目**：点击该按钮，您可以删除当前已设的所有过滤条目。

5.7.4.1 添加或编辑 MAC 地址过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面，界面中各参数说明见前面MAC地址过滤条目表中所述。

MAC地址过滤

本页通过MAC地址过滤来控制局域网中计算机对Internet的访问。

MAC 地址： 00-13-8F-A9-E6-CB

描 述： 张三的计算机

状 态： 生效

保 存 返 回 帮 助

举例:

设置局域网中MAC地址为00-13-8F-A9-E6-CB和 00-13-96-6B-6E-A9的计算机不能访问Internet，局域网中的其它计算机能访问Internet，这时您需要设置如下的MAC地址过滤表。

设置步骤:

首先在“防火墙设置”中打开防火墙总开关，然后开启“MAC地址过滤”，设置“缺省过滤规则”为“禁止已设MAC地址列表中已启用的MAC地址访问Internet，允许其它MAC地址访问Internet”。然后，点击添加新条目按钮，类似上面界面所示设置各条目参数，设置完后点击保存。最后形成的MAC地址过滤条目表为:

ID	MAC地址	描 述	状 态	配 置
1	00-13-8F-A9-E6-CB	张三的计算机	生效	编辑 删除
2	00-13-96-6B-6E-A9	李四的计算机	生效	编辑 删除

5.7.5 攻击防护

选择安全设置下的攻击防护，您将进入下面的攻击防护的设置界面。攻击防护是防火墙通过对数据包的检查，以应对一些恶意的攻击。攻击检查和防护分为四类:

- 扫描类攻击防护
- 拒绝服务（DoS）攻击防护
- 可疑包攻击防护
- 含有IP选项的包的攻击防护

如果在数据包中查到符合指定的攻击模式，则进行相应的防护处理。设置界面如下图所示。

攻击防护

区域： LAN

扫描类攻击防护：

- [ ] IP扫描 阈值：5000 微秒
- [ ] 端口扫描 阈值：5000 微秒
- [ ] IP欺骗

DoS类攻击防护：

- [ ] ICMP Flood 阈值：1000 PPS
- [ ] UDP Flood 阈值：1000 PPS
- [ ] SYN Flood 阈值：200 PPS
- [ ] Land Attack
- [ ] WinNuke

可疑包类防护：

- [ ] 大的ICMP包（大于1024字节）
- [ ] 没有flag的TCP包
- [ ] 同时设置SYN和FIN的TCP包
- [ ] 仅设置FIN而没有设置ACK的TCP包
- [ ] 未知协议

含有IP选项的包防护：

- [ ] IP Timestamp Option
- [ ] IP Security Option
- [ ] IP Stream Option
- [ ] IP Record Route Option
- [ ] IP Loose Source Route Option
- [ ] IP Strict Source Route Option
- [ ] 非法IP选项

保 存 帮 助

5.7.6 区域设置

区域设置表明，后续的攻击防护设置项，是对应来自指定区域的数据包进行监控。如选中LAN，则表示对来自局域网的数据包进行监控，如上图：

5.7.6.1 扫描类攻击防护

扫描类攻击防护包括三种类型：IP扫描、端口扫描、IP欺骗。

IP扫描

该项用来检查在小于规定的时间内，是否存在从一个源IP地址发送ICMP请求包到10个不同的目的IP地址的现象。如果有，则认为此源IP正在进行IP扫描攻击。选中IP扫描复选框，表明对来自指定区域（见区域设置节）的包进行IP扫描攻击的检查，设置阈值指明规定的时间间隔。阈值选择范围为2000-1000000微秒。如果欲取消对来自指定区域的包进行IP扫描攻击的检查，则清除IP扫描选择即可。

端口扫描

该项用来检查在小于规定的时间内，是否存在从一个源IP地址发送TCP SYN包到同一目的地址的10个不同端口的现象。如果有，则认为此源IP正在进行端口扫描攻击。选中端口扫描复选框，表明对来自指定区域的包进行端口扫描攻击检查，设置阈值指明规定的时间间隔，阈值选择范围为2000-1000000微秒。如果欲取消对来自指定区域的包进行端口扫描攻击检查，则清除端口扫描选择即可。

IP欺骗（仅针对局域网）

发出攻击的主机通常使用假IP地址作为自己的源地址，从而使得被攻击方不能查到真正的攻击者。选中IP欺骗复选框，表明对来自指定区域的包进行IP欺骗检查。如果欲取消对来自指定区域的包进行IP欺骗检查，则清除IP欺骗选择即可。

 注意:

本功能仅在区域为LAN时有效，在区域为WAN时是无效的。

5.7.6.2 DoS 类攻击防护

DoS类攻击防护包括五种类型：ICMP Flood、UDP Flood、SYN Flood、Land Attack、WinNuke。

ICMP Flood攻击

该项用来检查在一秒钟内，一个目的IP是否收到超过规定数量的ICMP请求包。如果收到超过规定数量的包，则认为此目的IP正受到ICMP Flood的攻击。选

中ICMP Flood复选框，表明对来自指定区域的包进行ICMP Flood攻击检查。设置阈值指明一秒内收到的包数（Packets Per Second），其范围为10-99999 PPS。如果欲取消对来自指定区域的包进行ICMP Flood攻击检查，则清除ICMP Flood选择即可。

UDP Flood攻击

该项用来检查在一秒钟内，一个目的IP的某一端口是否收到超过规定数量的UDP包。如果收到超过规定数量的包，则认为此目的IP的此端口正受到UDP Flood的攻击。选中UDP Flood复选框，表明对来自指定区域的包进行UDP Flood攻击检查。设置阈值指明一秒内收到的包数，范围为10-99999 PPS。如果欲取消对来自指定区域的包进行UDP Flood攻击检查，则清除UDP Flood选择即可。

SYN Flood攻击

该项用来检查在一秒钟内，一个目的IP的某一端口是否收到超过规定数量的TCP SYN包。如果收到超过规定数量的包，则认为此目的IP的此端口正受到SYN Flood的攻击。选中SYN Flood复选框，表明对来自指定区域的包进行SYN Flood攻击检查。设置阈值指明一秒内收到的包数，范围为10-99999 PPS。如果欲取消对来自指定区域的包进行SYN Flood攻击检查，则清除SYN Flood选择即可。

LAND攻击

该项用来检查将SYN Flood攻击和IP欺骗结合在一起的攻击，当攻击者发送含有受害者IP地址的欺骗性SYN封包，将其作为目的和源IP地址时，就发生了LAND攻击。选中LAND Attack复选框，表明对来自指定区域的包进行Land 攻击检查。如果欲取消对来自指定区域的包进行LAND攻击检查，则清除LAND Attack选择即可。

WinNuke

WinNuke是针对网上运行Windows的任何计算机的DoS攻击。攻击者将TCP片段（通常给设置了紧急[URG]标志的NetBIOS端口139）发送给已建连接的主机。这样就产生NetBIOS碎片重叠，从而导致运行Windows的机器崩溃。选中WinNuke复选框，表明对来自指定区域的包进行WinNuke攻击检查。如果欲取消对来自指定区域的包进行WinNuke攻击检查，则清除WinNuke选择即可。

5.7.6.3 可疑包类防护

可疑包类防护包括五类：大的ICMP包（大于1024字节）、没有Flag的TCP包、同时设置SYN和FIN的TCP包、仅设置FIN而没有设置ACK的TCP包、未知协议。

大的ICMP包（大于1024字节）

正常的ICMP数据包长度较小，一般不会大于1024字节。选中大的ICMP包（大于1024字节）复选框，表明对来自指定区域的包进行ICMP包合法性检查。如果欲取消对来自指定区域的包进行大的ICMP包（大于1024字节）检查，则清除相应选项的选择即可。

没有Flag的TCP包

正常的TCP包的包头至少设置有一个标志（flag）。未设置任何控制标志的TCP包是一个可疑包。选中没有Flag的TCP包复选框，表明对来自指定区域的包进行没有Flag的TCP包检查。如果欲取消对来自指定区域的包进行没有Flag的TCP包检查，则清除相应选项的选择即可。

同时设置SYN和FIN的TCP包

TCP包头的SYN标志同步发起TCP连接的序列号，FIN标志表示完成TCP连接的数据传输的结束。两个标志的用途是互相排斥的。在同一TCP片段包头中同时设置SYN和FIN控制标志是异常的TCP包。选中同时设置SYN和FIN的TCP包复选框，表明对来自指定区域的包进行同时设置SYN和FIN的TCP包检查。如果欲取消对来自指定区域的包进行同时设置SYN和FIN的TCP包检查，则清除相应选项的选择即可。

仅设置FIN而没有设置ACK的TCP包

含有ACK标志的TCP包是确认接收到的前一个包。含有FIN标志的TCP包是发送会话结束信号并终止连接，它通常也设置了ACK标志。设置了FIN标志，而未设置 ACK标志的TCP包是异常的TCP包。选中仅设置FIN而没有设置ACK的TCP包复选框，表明对来自指定区域的包进行仅设置FIN而没有设置ACK的TCP包检查。如果欲取消对来自指定区域的包进行仅设置FIN而没有设置ACK的TCP包检查，则清除相应选项的选择即可。

未知协议

目前，IP包头的协议类型（protocol type）字段保留大于135（包括135）的数值未定义。正是由于这些协议未定义，就无法事先知道某一特定的未知协议是善意的还是恶意的。对这些非标准协议，谨慎的态度是封锁这类未知的元素进入受保护网络。选中未知协议复选框，表明对来自指定区域的包进行未知协议检查。如果欲取消对来自指定区域的包进行未知协议检查，则清除相应选项的选择即可。

5.7.6.4 含有 IP 选项的包防护

在Internet Protocol 协议（RFC 791）中，指定了一组选项以提供特殊路由控制、诊断工具和安全性。它是在IP包头中的目的地址之后。协议认为这些选项“对最常用的通信是不必要的”。在实际使用中，它们也很少出现在IP包头中。这些选项经常被用于某些恶意用途。

IP选项包括:

- **IP Timestamp Option**：表明是否检查来自指定区域的IP包含有Internet Timestamp项
- **IP Security Option**：表明是否检查来自指定区域的IP包含有Security项
- **IP Stream Optio**n：表明是否检查来自指定区域的IP包含有Stream ID项
- **IP Record Route Optio**n：表明是否检查来自指定区域的IP包含有Record Route项
- **IP Loose Source Route Option**：表明是否检查来自指定区域的IP包含有Loose Source Route项
- **IP Strict Source Route Option**：表明是否检查来自指定区域的IP包含有Strict Source Route项
- **非法IP选项**：表明是否检查来自指定区域的IP包的完整性或正确性

选中一项IP选项的复选框，则检查；清除选项的选择，则取消检查。

5.8 路由功能

- 路由功能
  - 静态路由表

在“路由功能”菜单下面，只有“静态路由表”一个子项。单击该子项，您即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

5.8.1 静态路由表

选择路由功能下的静态路由表项，您将进入下面所示界面。本页设置路由器的静态路由功能，您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。


静态路由表

本页设置路由器的静态路由信息。

ID	目的IP地址	子网掩码	网关	状态	配置
1	222.99.99.220	255.255.255.0	222.88.88.1	失效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

- **静态路由表**：显示静态路由条目表中的信息。
  - **目的IP地址** 显示欲访问的主机的IP地址。
  - **子网掩码**：显示子网掩码，一般为255.255.255.0。
  - **网关**：显示数据包被发往的路由器或主机的IP地址。
  - **状态**：显示本条目的状态，即本条目是否生效。
  - **配置**：显示对本条目操作的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以在路由列表中添加新的条目。
- **使所有条目生效**：点击该按钮，您可以将列表中所有条目的状态设为“生效”。
- **使所有条目失效**：点击该按钮，您可以将列表中所有条目的状态设为“失效”。
- **删除所有条目**：点击该按钮，您可以删除当前列表中已设的所有条目。

当您点击“添加新条目”或点击“编辑”链接界面时，您将进入下面的设置界面。您可以参照图中各参数，正确设置您需要的路由条目。

静态路由表

本页设置路由器的静态路由信息。

目的IP地址： 222.99.99.220
子网掩码： 255.255.255.0
默认网关： 222.88.88.1
状态： 失效

保 存 返 回 帮 助

5.9 连接数限制

- 连接数限制
  - 连接数设置
  - 连接数列表

在“连接数限制”菜单下面，共有“连接数设置”、“连接数列表”两个子项。

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.9.1 连接数设置

选择连接数限制下的连接数设置，您将进入连接数设置界面。本页设置单机的连接数限制，对指定IP地址的计算机连接数进行限制，超过限制的新连接不允许通过路由器，未设置限制的计算机可以不受限制的建立连接。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。如下图示:



连接数设置

本页设置单机的连接数限制。

连接数限制： 不启用 启用 保 存

ID	局域网IP地址	最大连接数	启用	配置
1	192.168.1.10-192.168.1.30	200	☑	编辑 删除
2	192.168.1.40	100	☑	编辑 删除

添加新条目 删除所有条目

上一页 下一页 帮 助

➢ **连接数限制**：您可以选择是否开启连接数限制功能。

➢ **连接数限制列表**：显示已经设置的连接数限制条目。

➢ **局域网IP地址**：显示您希望限制的计算机的IP地址。可以输入一个IP地址段，例如：192.168.1.20-192.168.1.30，也可以只输入一个IP地址，例如：192.168.1.40。

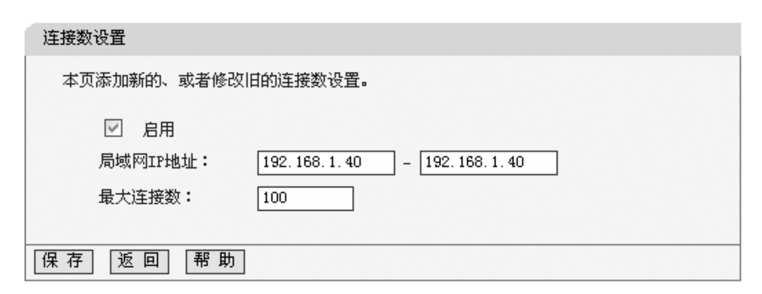
➢ **最大连接数**：显示允许该计算机建立的最大连接数。

➢ **启用**：显示该条目的限制是否生效。

➢ **添加新条目**：点击该按钮，您可以在列表中添加新的条目。

➢ **删除所有条目**：点击该按钮，您可以删除列表中的所有条目。

当您点击"添加新条目"或点击"编辑"链接时的界面时，您将进入下面的设置界面。在该界面中您可以添加一条新的连接数限制条目，也可以编辑已经存在的限制条目。



5.9.2 连接数列表

选择连接数限制下的连接数列表，您将进入下面所示界面。本页显示已设置的连接数和当前通过路由器的所有连接数，下图只显示了连接数列表中的部分数据。

连接数列表

本页显示连接数列表。
局域网地址总数：22　　当前总连接数：1

ID	局域网IP地址	最大连接数	当前连接数
1	192.168.1.23	200	1
2	192.168.1.11	200	0
3	192.168.1.10	200	0
4	192.168.1.13	200	0
5	192.168.1.12	200	0
6	192.168.1.15	200	0

- **局域网IP地址**：客户端的IP地址。
- **最大连接数**：设定的连接数限制，如果没有设置限制则显示“无限制”。
- **当前连接数**：该客户端当前有效的连接数。

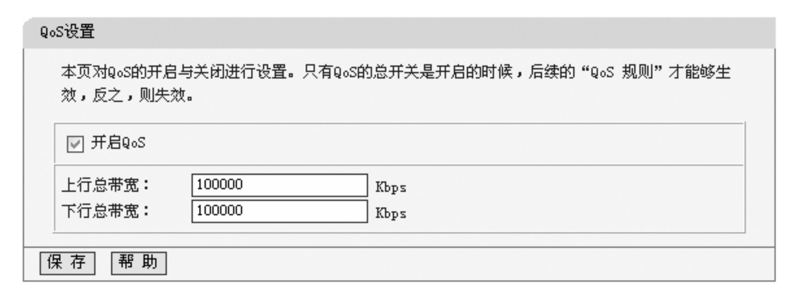
5.10 QoS

- QoS
  - QoS设置
  - QoS规则

在“QoS”菜单下面，共有“QoS设置”、“QoS规则”两个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.10.1 QoS 设置

选择QoS下的QoS设置，您将进入下面所示界面。本页主要对QoS的开启与关闭进行设置。



- **开启功能**：请您选择是否开启QoS设置，选中该复选框则表示启用该功能。
- **上行总带宽**：请您输入希望路由器通过WAN口提供的上传速率，最大值为100000Kbps。
- **下行总带宽**：请您输入希望路由器通过WAN口提供的下载速率，最大值为100000Kbps。



注意：

只有QoS的总开关开启时，后续的“QoS 规则”才能够生效，反之，则无效。

5.10.2 QoS 规则

选择QoS下的QoS规则，您将进入下面所示界面。QoS规则分为QoS规则列表和QoS规则配置。


QoS规则列表

本页为QoS规则列表。

ID	描述	模 式	上行带宽(Kbps)		下行带宽(Kbps)		启 用	配 置
			最小	最大	最小	最大		
1	192.168.1.10 - 192.168.1.250/80 - 85/TCP	独立	400	1000	400	1000	☑	编辑 删除

添加新条目 删除所有条目

上一页 下一页 当前第 1 页 帮 助

在QoS规则列表中，可以查看用户创建的全部规则。每个规则包含的条目有:

- **QoS规则列表**：显示用户创建的所有规则信息。每个规则包含的条目有：
  - **ID**：规则序号。
  - **描述**：显示描述的信息，包括地址段，传输层的端口段和协议；其格式有：地址段/端口段/协议，端口段/协议，端口段，地址段。
  - **模式**：显示带宽的使用形式，分为独立带宽和共享带宽；独立带宽表示地址或端口各自拥有上下行带宽值，共享带宽表示地址或端口共享上下行带宽值。
  - **上行带宽**：显示WAN口允许的最大上传速度限制和最小上传速度保证，为0时表示上行总带宽。输入范围为0-100000Kbps。
  - **下行带宽**：显示WAN口允许的最大下载速度限制和最小下载速度保证，为0时表示下行总带宽。输入范围为0-100000 Kbps。
  - **启用**：显示规则的状态，选中该复选框则表示该规则生效。
  - **配置**：显示可以对该规则进行的超级链接——编辑或删除。
- **添加新条目**：点击该按钮，您可以添加新的QoS规则。
- **删除所有条目**：点击该按钮，您可以删除列表中的所有规则条目。

当您点击QoS规则列表中的添加新条目或编辑按钮时，您将进入下面的设置界面。在QoS规则配置中，您可以创建新的QoS规则或修改已存在的规则。具体设置见下图示。

QoS规则配置

本页通过QoS规则来进行带宽控制。

☑ 启用

地址段： 192.168.1.10 - 192.168.1.250

端口段： 80 - 85

协 议： TCP （只有选中端口段，该域才有效）

模 式： 独立带宽

	最小带宽（Kbps）	最大带宽（Kbps）
上 行：	400	1000
下 行：	400	1000

保 存 返 回 帮 助

- **启用**：请您选择是否启用该规则。
- **IP地址段**：请您输入内部主机的地址范围。当全部为空或为0.0.0.0时表示该域无效。
- **端口段**：请您输入内部主机访问外部服务器的端口范围。当全部为空或为0时表示该域无效。
- **协议**：请您输入传输层采用的协议类型，这里有ALL(任意匹配)、TCP和UDP；该域只有在端口段选中下才有效。
- **模式**：请您选择该条规则下，带宽使用的模式，即独立或共享带宽。
- **上行带宽、下行带宽**：请您参考QoS规则列表中所述来设置。

5.11IP 与 MAC 绑定

- IP与MAC绑定
  - 静态ARP绑定设置
  - ARP映射表

在“IP与MAC绑定”的菜单下面，有“静态ARP绑定设置”、“ARP映射表”两个子项。单击某个子项，您即可进行相应功能的设置，下面将详细讲解各个子项的功能。

5.11.1 静态 ARP 绑定设置

选择IP与MAC绑定下的静态ARP绑定设置，即可进入该项的设置界面。ARP绑定是指，指定的IP地址的主机在向路由器发送arp请求时，当MAC地址与绑定

的MAC地址相同时，才允许其通过路由器，否则不允许使用该IP地址的主机发送的arp请求通过路由器。

本页显示已经设置的ARP静态列表。您可以利用按钮“增加单个条目”来增加新的ARP静态条目，或者通过按钮“编辑”或“删除”链接来修改或删除旧的ARP静态条目。

要使用ARP绑定功能，您需要先设置以下项目：

静态ARP绑定设置

本页设置单机的MAC地址和IP地址的匹配规则

ARP绑定： ◉不启用 ○启用 保 存

ID	MAC地址	IP地址	绑定	配置
1	00-13-8F-A9-E6-CA	192.168.1.100	☑	编辑 删除

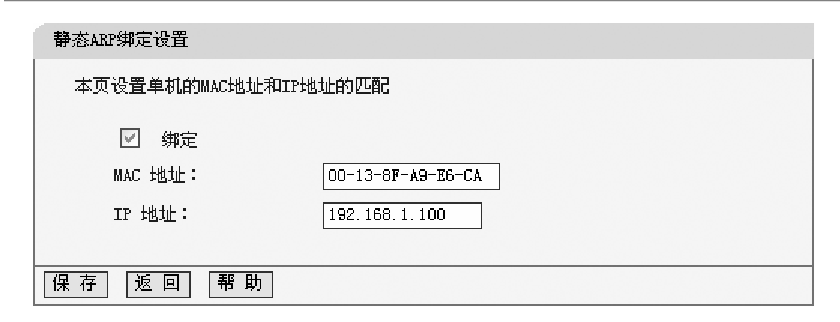
增加单个条目 使所有条目生效 删除所有条目 查找指定条目

上一页 下一页 当前第 1 页 帮 助

- **ARP绑定**：请您选择是否开启ARP绑定功能。选择启用并按下按钮“保存”后，ARP绑定功能才能生效。
- **静态ARP绑定列表**：显示IP与MAC地址绑定的条目信息。
  - **MAC地址**：显示您希望控制的计算机的MAC地址。
  - **IP地址**：显示您希望与指定MAC地址绑定的IP地址。
  - **绑定**：显示该条目的状态，选中该复选框则表示绑定条目生效。
  - **编辑**：显示对该绑定条目操作的超级链接——编辑或删除。
- **增加单个条目**：点击该按钮，您可以在静态绑定列表中添加新的条目。
- **删除所有条目**：点击该按钮，您可以删除静态列表中的所有条目。
- **查找指定条目**：点击该按钮，您可以在静态列表中查找指定IP地址或MAC地址的条目。具体查找方法见后面所述。
- **使所有条目生效**：点击该按钮，您可以使当前静态列表中的所有绑定条目生效。

5.11.1.1 添加或编辑静态 ARP 绑定条目

当您需要添加或编辑静态ARP绑定条目时，请点击上图所示界面中的“增加单个条目”或“编辑”按钮，您可以进入下面的设置界面。



举例:

设置只允许局域网中MAC地址为00-13-8F-A9-E6-CA的计算机使用IP地址192.168.1.100。

设置步骤:

首先，请设置该节首页中的“ARP绑定”为启用，并保存。

然后请点击 “增加单个条目”按钮，并按上图设置添加新的静态绑定条目。最后按下保存即可。

您也可以通过条目上配置中的“编辑”按钮，对已经设置的条目进行编辑，其界面与上图相同。

5.11.1.2 查找静态 ARP 绑定条目

如果您希望查找特定的IP地址或MAC地址是否已经设置到静态绑定表中，您可以在首页中点击“下一页”、“上一页”按钮或直接选择指定页进行浏览查找。另外，您也可以点击按钮“查找指定条目”进入到下图界面中进行快速查找。

静态ARP条目查找

查找指定MAC地址和(或)IP地址的静态绑定条目

MAC 地址： 00-13-8F-A9-E6-CA

IP 地址：

查 找

ID	MAC地址	IP地址	绑定	链接
当前查找结果为空				

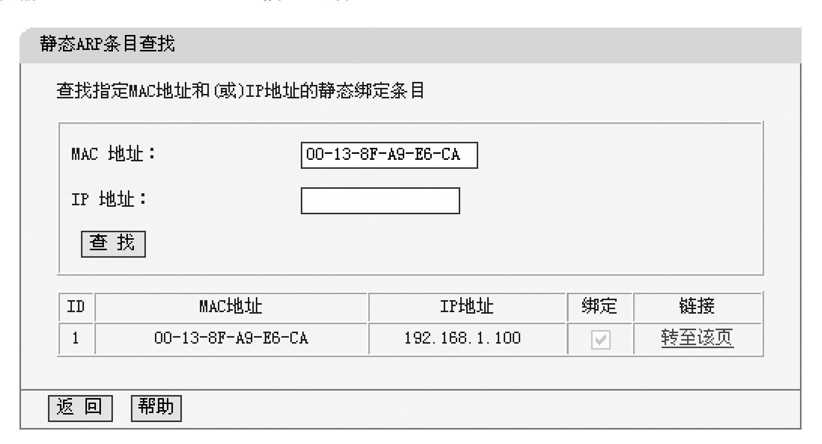
返 回 帮助

举例:

例如您要查找IP地址为192.168.1.23的条目。

查找步骤如下:

首先，请单击按钮“查找指定条目”，然后进入下图设置查找信息，您可以直接输入MAC地址或IP地址信息进行查找。



最后，单击按钮“查找”，则可以得到结果。

在上图中，如果您需要对该条目进行进一步的编辑操作，可以点击上图所示界面中的链接——“转至该页”按钮，进入该条目所在的ARP静态绑定列表所在页

（条目呈高亮），再选择条目旁边的“编辑”按钮，进入编辑界面对它进行编辑。如下图示:

静态ARP绑定设置

本页设置单机的MAC地址和IP地址的匹配规则

ARP绑定： ◉不启用 ○启用 保 存

ID	MAC地址	IP地址	绑定	配置
1	00-13-8F-A9-E6-CA	192.168.1.100	☑	编辑 删除

增加单个条目 使所有条目生效 删除所有条目 查找指定条目

上一页 下一页 当前第 1 页 帮 助

5.11.2 ARP 映射表

选择IP与MAC绑定下的ARP映射表，您可以进入ARP映射表显示界面。本页显示当前设置的和通过路由器ARP的映射列表，并显示是否已经绑定。同时也可以将指定映射条目导入到ARP静态列表中进行进一步的编辑操作，或者直接删除该映射条目。



- **ARP映射表**: 显示映射表条目信息。
  - **MAC地址**: 显示网络中计算机的MAC地址。
  - **IP地址**: 显示与MAC地址匹配的计算机的IP地址。
  - **状态**: 显示该条目状态，绑定或未绑定。
- **配置**: 显示对该条目的操作的超级链接——导入或删除。
  - **导入**: 点击该按钮，您可以将该条目导入到前面的静态ARP绑定列表中。
  - **删除**: 点击改按钮，您可以将该条目从ARP映射表中删除。

⚠ 注意:

1 删除时，如果该条目状态为“已绑定”，且在静态ARP绑定列表中该条目也已经绑定，则会使该静态绑定条目的状态由绑定变成不绑定。

2 上面 1 情形必须在静态ARP绑定设置启用时才起作用。

- **全部绑定**: 点击该按钮，您可以动态绑定当前列表中所有条目(不保存到静态ARP绑定列表中)。
- **全部导入**: 点击改按钮，您可以把当前ARP映射表的所有条目全部导入到静态ARP绑定列表中，如果有冲突条目，将忽略冲突条目，添加其他条目；如果静态绑定表已满，则忽略多余的条目。

5.12动态 DNS

DDNS的功能是实现固定域名到动态IP地址之间的解析。对于使用动态IP地址的用户，在每次上网得到新的IP地址后，安装在主机上的动态域名软件就会把该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。Internet上的其他人要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。这样，针对大多数不使用固定IP地址的用户，通过动态域名解析服务就可以经济、高效的构建自身的网络系统。

花生壳DDNS服务提供者是www.oray.net；科迈网DDNS服务提供者是www.comexe.cn。在注册成功后，用注册时的用户名和密码就可以登录到DDNS服务器上。当连接状态显示成功之后，互联网上的其它主机就可以通过以域名的方式对您的路由器或虚拟服务器进行访问了。

5.12.1 花生壳 DDNS

选择动态DNS菜单，在界面的“服务提供者”下拉选项中选择“花生壳（www.oray.net）”，您将进入下图所示的花生壳DDNS设置界面。本页设置“花生壳”的DDNS参数，当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式对您的路由器或虚拟服务器进行访问了。

动态DNS设置

本页设置“Oray.net花生壳DDNS”的参数。

服务商链接：花生壳动态域名解析服务申请　花生壳动态域名解析服务帮助

服务提供者：花 生 壳（www.oray.net）

WAN口：WAN 口 1

用户名：

密 码：

启用DDNS：

连接状态：DDNS 未启动

服务类型：- - -

域名信息：NULL

登 录　退 出

保 存　帮 助

- **服务商链接**：当您成功连接外网后，点击该项，您可以分别链接到“花生壳动态域名解析服务申请”和“花生壳动态域名解析服务帮助”页面。
- **服务提供者**：请您选择提供DDNS的服务器名。
- **WAN口**：请您选择向DDNS服务器注册使用的WAN口（WAN1或WAN2）。
- **用户名**：请您输入在DDNS服务器上注册的用户名。
- **密　码**：请你输入在DDNS服务器上注册的密码。
- **启用DDNS**：请您选择是否启用该DDNS功能。
- **连接状态**：显示当前与DDNS服务器的连接状态。
- **服务类型**：显示用户的类型（花生壳专业用户或者花生壳标准用户）。
- **域名信息**：显示当前DDNS服务器获得的域名服务列表。

5.12.2 科迈 DDNS

选择动态DNS菜单，在界面的“服务提供者”下拉选项中选择“科迈网（www.comexe.cn）”，您将进入下图所示的科迈网DDNS设置界面。本页设置“科迈网”的DDNS参数。当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式对您的路由器或虚拟服务器进行访问了。

动态DNS设置

本页设置动态DNS参数

服务提供者： 科 迈 网（www.comexe.cn） 注册...
域名：
域名：
域名：
域名：
域名：

WAN口： WAN 口 1

用户名：
密 码：

启用DDNS：
连接状态： DDNS 未启动

登 录 退 出

保 存 帮 助

- **服务提供者**：请您选择提供DDNS的服务器名。
- **域名**：请您输入在DDNS服务器上已经注册的域名信息。
- **WAN口**：请您选择向DDNS服务器注册使用的WAN口（WAN1或WAN2）。
- **用户名**：请您输入在DDNS服务器上注册的用户名。
- **密码**：请您输入在DDNS服务器上注册的密码。
- **启用**：请您选择是否启用该DDNS功能。
- **连接状态**：显示当前与DDNS服务器的连接状态。

5.13 交换机功能

- 交换机功能
  - 端口统计
  - 端口监控
  - 端口流量限制
  - 端口参数
  - 端口状态
  - Port VLAN

在"交换机功能"菜单下面，共有"端口统计"、"端口监控"、"端口流量限制"、"端口参数"、"端口状态"、"Port VLAN"六个子项。单击某个子项，您即可进行相应的功能设置或查询相关的状态，下面将详细讲解各子项的功能。

5.13.1 端口统计

选择交换机功能下的端口统计，您可以进入端口统计显示界面。端口统计将针对每一个端口，统计它收发了多少数据字节、多少数据帧、多少个广播帧、多少个多播帧、多少个错误帧等等。其页面显示如下:

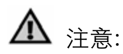
端口统计

当前端口：端口1　　刷 新　　清 空　　帮 助

Rx Unicasts：	2487	Tx Unicasts：	2732
Rx Broadcasts：	96	Tx Broadcasts：	28
Rx Multicasts：	28	Tx Multicasts：	0
Rx Bytes：	406646	Tx Bytes：	1392601
Rx Pauses：	0	Tx Pauses：	0
Rx CRC Errors：	0	Rx Collisions：	0
Rx 64 B：	1702	Rx 65to127 B：	252
Rx 128to255 B：	55	Rx 256to511 B：	449
Rx 512to1023 B：	153	Rx 1024toMax：	0
Rx Undersizes：	0	Rx Fragments：	0
Rx Oversizes：	0	Rx Jabbers：	0

- **Rx Unicasts**: 接收的数据帧的目的MAC地址为单播MAC地址的数据帧数目。
- **Tx Unicasts**: 发送的数据帧的目的MAC地址为单播MAC地址的数据帧数目。
- **Rx Broadcasts**: 接收的数据帧的目的MAC地址为广播MAC地址的数据帧数目。
- **Tx Broadcasts**: 发送的数据帧的目的MAC地址为广播MAC地址的数据帧数目。
- **Rx Multicasts**: 接收的数据帧的目的MAC地址为多播MAC地址的数据帧数目。
- **Rx Bytes**: 接收的数据帧的总字节数（不包含错误帧）。
- **Tx Bytes**: 发送的数据帧的总字节数（不包含错误帧）。
- **Rx Pauses**: 接收的Pause帧的数据帧数目。
- **Tx Pauses**: 发送的Pause帧的数据帧数目。

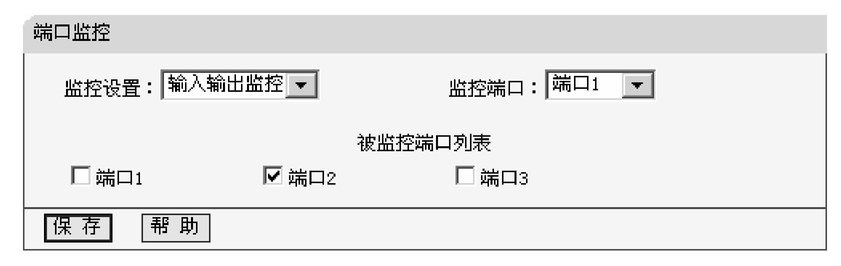
- **Rx CRC Errors**: 接收的含非法校验字段的数据帧数目。
- **Rx Collisions**: 接收数据帧时产生的碰撞（即冲突）数目。
- **Rx 64 B**: 接收及转发的长度为64字节的数据帧数目（包含错误帧）。
- **Rx 65 to127** ：接收及转发的长度为65～127字节的数据帧数目（包含错误帧）。
- **Rx 128 to255 B**: 接收及转发的长度为128～255字节的数据帧数目（包含错误帧）。
- **Rx 256 to511 B**: 接收及转发的长度为256～511字节的数据帧数目（包含错误帧）。
- **Rx 512 to1023 B**: 接收及转发的长度为512～1023字节的数据帧数目（包含错误帧）。
- **Rx 1024 toMax**: 接收及转发的长度为1024～1518字节的数据帧数目（包含错误帧）。
- **Rx Undersizes**: 接收的长度小于64字节并且包含合法校验字段的数据帧数目。
- **Rx Fragments**: 接收的长度小于64字节并且包含非法校验字段的数据帧数目。
- **Rx Oversizes**: 接收的长度超过最大字节数并且包含合法校验字段的数据帧数目。
- **Rx Jabbers**: 接收的长度超过最大字节数并且包含非法校验字段的数据帧数目。



以太网中的数据帧长度一般在64到1522字节之间，本交换机支持最大帧长为1522（IEEE Tag帧）或1518（untag帧）的数据帧的统计，超出这个长度的数据帧将被统计成错误帧（Jumbo帧除外）。

5.13.2 端口监控

选择交换机功能下的端口统计，您可以进入如下端口监控界面。端口监控主要是使用一个监控端口对一个或多个被监控端口进行输入监控（Ingress），输出监控（Egress）或输入输出监控（Ingress & Egress）。这里的输入/输出是相对路由器的交换机部分而言的。



- **监控模式**: 请您选择端口监控的模式：禁用、输入监控、输出监控或输入输出监控。这里的输入/输出是相对路由器的交换机部分而言的。
- **监控端口**: 请您选择监控主机的端口。

➢ **被监控端口**：请您选择被监控端口。



注意:

1 MR904B仅支持输出监控和输入输出监控。

2 端口监控不支持跨越VLAN的监控，当设置多个VLAN时，注意要将监控端口添加到需要被监控的端口成员所在的VLAN中。

5.13.3 端口流量限制

选择交换机功能下的端口流量限制，您可以进入如下设置界面。端口流量限制提供针对每个端口的流量限制设置，入口提供“不限制”、“FLOOD”、“广播和多播”、“广播”、“所有帧”等五种不同的限制模式，而出口限制则是针对所有帧的限制。



➢ **入口限制模式**：请您选择入口限制模式，它一共包含下面五个选项。

- **不限制**：选择该项表示对进入该端口的数据帧不进行限制。
- **FLOOD**：选择该项表示对进入该端口的广播帧、多播帧、以及目的MAC地址不在MAC地址表的帧进行限制。
- **广播和多播**：选择该项表示对进入该端口的广播帧和多播帧进行限制。
- **广播**：选择该项表示对进入该端口的广播帧进行限制。
- **所有帧**：选择该项表示对进入该端口的所有帧进行限制。

其中FLOOD、广播以及广播和多播的限制方式就是传统意义上的广播风暴抑制，路由器的交换机部分可以对三种常见的广播帧（广播包、组播包、未学习到地址的单播包）进行过滤。

广播风暴是指网络上的广播帧数量急剧增加而影响正常的网络通讯的反常现象。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧，广播风暴会严重降低网络性能。端口流量限制允许交换机部分对网络上出现的广播帧进行过滤。当交换机检测到广播帧数目超出一定的范围时，会自动丢弃广播帧，以防止广播风暴的发生。

当设置为所有帧的限制方式时，交换机部分将对所有的数据帧都进行限制，对于入口的数据包采用过滤处理，若当前流量超出入口限制流量时，超出的部分将被丢弃；对于出口的数据，仅限制流量（根据端口流量控制的开启情况决定是否丢弃超出限制速率外的帧），这时起到端口下行带宽限制的作用。


注意:

在限制速率的设置上，MR904B仅支持分级的设置，即只能从已有选项中选择速率。

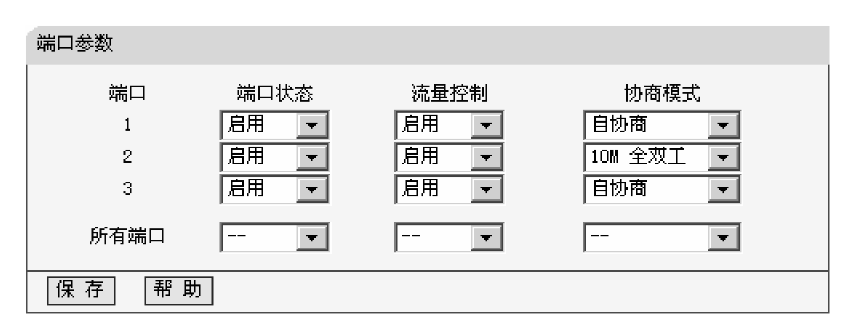
5.13.4　端口参数

选择交换机功能下的端口参数，您可以进入如下设置界面。它主要包括是否启用端口，是否启用端口流量控制，以及设置端口工作模式。

➢ **端口的工作模式**

MR904B的交换机部分支持五种端口工作模式：10M半双工，10M全双工，100M半双工，100M全双工和自协商模式。

如100M全双工，前面的数字表示的是传输速率，后面表示的是双工模式。半双工是指传输的两边既可以发送，也可以接收，但是在某一时刻只能有一个设备使用网络传输介质，即不能同时进行发送和接收；全双工是指传输的两边可以同时进行发送和接收，互不影响。



➢ **端口的N-Way自动协商功能**

交换机部分的端口提供N-Way自协商功能。该功能使交换机的端口可根据另一端设备的连接速度和双工模式，自动调节速度和双工模式到双方都可以达到的最高水平。自协商的设备可以交换关于各自功能的信息，这样就可以使设备进行自动配置，实现自动调整传输方式（全双工或半双工）和传输速度（10Mbps，100Mbps，1000Mbps）的功能。

➢ **流量控制**

流量控制（Flow control）是为了同步接收方和发送方的的速度而进行的控制。当接收方接收能力比发送方的发送能力小的时候，如果没有流量控制就会丢失数据。流量控制主要分两种情况：在半双工方式下，流控采用Backpressure标准；在全双工方式下，使用基于PAUSE帧的流量控制，即IEEE802.3x标准。

半双工方式下，当接收方设备的资源不足时就会启动流量控制，发送一组载波信号脉冲串（假冲突信号），发送方设备检测到网络上的载波信号和自己发送的信号不同，就会停止一段时间（随机时间）后再发送数据，接收方就可以在这个时间内处理数据，从而达到流量控制。

全双工方式下，当接收方设备的资源不足时就会启动流量控制。由于发送方发送数据时接收方也可以发送数据给发送方（全双工的特征），因此接收方可以通过发送一个PAUSE帧告诉发送方停止一段时间再发送数据。这就是全双工下流量控制下的IEEE802.3x 标准。

5.13.5 端口状态

选择交换机功能下的端口参数，您可以进入如下端口状态显示界面。端口状态可以标识端口上是否接有设备，如果接有设备，它的工作速率是多少，它是工作在全双工模式还是半双工模式，它是否启用了流量控制等等。

端口状态

端口	端口状态	连接速率(Mbps)	双工模式	流量控制
1	已连接	100	全双工	启用
2	未连接	--	--	--
3	未连接	--	--	--

刷新

5.13.6 Port VLAN

选择交换机功能下的Port VLAN，您可以进入Port VLAN的设置界面。虚拟局域网（Virtual Local Area Network，VLAN）可以把数据交换限制在各个虚拟网的范围内，从而减少整个网络范围内广播包的传输，提高网络的传输效率；同时各虚拟网之间不能直接进行通讯，而必须通过路由器转发，起到了隔离端口的作用，为高级安全控制提供了可能，增强了网络的安全性。VLAN功能的适用性很广，在数据交换较频繁或对网络安全性有要求的环境均可适用。如：1、在智能小区、校园、企业等应用环境，使用VLAN功能可使不同VLAN间的工作站不能互相访问，可为网络安全控制提供良好保障；2、在大型网吧、大中型企业等环境中，使用VLAN可大大减少网络中不必要的数据交换的数量，杜绝广播风暴，提升网络传输性能。并且，通过网络分段的方法，各个网段可共用一套网络设备，这样不仅减少了网络硬件的开销，还有利于设备迁移，降低连网成本。

本页显示当前VLAN的配置信息，MR904B支持3个VLAN的设置。缺省情况下，只有VLAN1是启用的，所有的端口成员都处于同一个VLAN中。当需要添加一个新的VLAN时，应先启用要设置的 VLAN，再按照自己的需要添加VLAN的成员端口。

Port VLAN 配置

端口		1	2	3
VLAN 1	☑ 启用	☑	☐	☑
VLAN 2	☑ 启用	☐	☑	☐
VLAN 3	☐ 启用	☐	☐	☐

清 空　保 存　帮 助

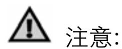
- **启用**：请您选择是否启用对应的VLAN设置，只有选择启用后，才能设置该VLAN。
- **VLAN1/2/3**：VLAN（虚拟局域网）的编号。
- **端口**：请您选择该VLAN的端口，它对应于路由器的物理端口，选中某端口，则表示此端口是该VLAN的成员，否则不是。

在您设置VLAN时，您需要遵循以下几条规则:

1）已启用的VLAN不允许存在VLAN包含关系;

2) 已启用的VLAN的端口成员不允许为空，允许单独一个端口构成一个VLAN;

3) 当前启用的VLAN条目不允许为空。

 注意:

当一个端口不属于任何一个VLAN时，它与单个端口独自构成一个VLAN时一致。

5.14系统工具

- 系统工具
  - 时间设置
  - 软件升级
  - 恢复出厂设置
  - 备份和载入配置
  - 重启路由器
  - 修改登录口令
  - 系统日志
  - 远端WEB管理
  - 流量统计
  - 联机测试
  - IP地址转换表
  - NAT源端口设置

在“系统工具”菜单下面，共有“时间设置”、“软件升级”、“恢复出厂设置”、“备份和载入配置”、“重启路由器”、“修改登录口令”、“系统日志”、“远端WEB管理”、“流量统计”、“联机测试”、“IP地址转换表”和“NAT源端口设置”共十二个子项。单击其中某个子项，即可对它进行相应的功能设置，下面将详细讲解各子项的功能。

5.14.1 时间设置

选择系统工具下的时间设置，您可以进入下面的时间设置界面。本页用来设置路由器的系统时间，您可以选择自己设置时间，也可以选择从互联网上获取标准的GMT时间。具体设置页面如下:

时间设置

本页设置路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的GMT时间。

注意：关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能（如防火墙）中的时间限定才能生效。

时区：（GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北

日期：2006 年 1 月 1 日

时间：10 时 52 分 40 秒

优先使用 NTP Server：0.0.0.0 0.0.0.0

获取GMT时间 （仅在连上互联网后才能获取GMT时间）

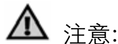
保 存 帮 助

➢ **优先使用NTP Server**：请您输入希望采用的NTP Server的IP地址（可以输入两个）。NTP Server是网络时间服务器，用于Internet网上的计算机时间同步。当路由器获取GMT时间时，优先从该时间服务器上获取。

设置步骤:

首先请您选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击保存按钮完成系统时间的设置。

如果您已经连上了互联网，则您也可以直接单击获取GMT时间按钮，从互联网上获取标准的GMT时间。


注意:

1 关闭路由器电源后，时间信息会丢失，只有当您下次开机连上Internet后，路由器才会自动获取GMT时间。

2 您必须先连上Internet获取GMT时间或在此页手动设置系统时间，路由器其他功能（如防火墙）中的时间限定才能生效。

5.14.2 软件升级

选择系统工具下的软件升级，您可以进入下面的软件升级界面。通过升级本路由器的最新版本软件，您将获得最新的功能。升级页面如下:

软件升级

通过升级本路由器的软件，您将获得新的功能。

文件： [ ] 浏览...

当前软件版本： 3.3.1 Build 070809 Rel.54595n
当前硬件版本： MR904BV1 00000000

注意：升级时请选择与当前硬件版本一致的软件。升级后路由器的设置可能会恢复出厂设置，请先备份配置文件。升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。当升级结束后，设备将会自动重新启动。

升 级

升级步骤:

- 请先登录本公司的网站(www.mercurycom.com.cn)，下载最新版本的软件。
- 选择系统工具下的软件升级项，在上图界面中的文件栏内填入已下载文件的全路径文件名，或用浏览按钮选择已下载的升级文件。
- 单击升级按钮进行软件升级。
- 升级完成后，路由器将自动重启。

 注意:

1 升级时请选择与当前硬件版本一致的软件。

2 在升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程需要一段时间，升级完成后，路由器将会自动重启。

5.14.3 恢复出厂设置

选择系统工具下的恢复出厂设置，您可以进入下面的操作界面。单击恢复出厂设置按钮将使路由器的所有设置恢复到出厂时的默认状态。操作页面如下:

恢复出厂设置

单击此按钮将使路由器的所有设置恢复到出厂时的默认状态。

恢复出厂设置

帮 助

出厂默认情况下的各参数如下:

- **默认的用户名**: admin
- **默认的密码**: admin
- **默认的IP地址**: 192.168.1.1
- **默认的子网掩码**: 255.255.255.0

恢复出厂设置后，路由器将自动重启。

5.14.4　备份和载入配置

选择系统工具下的备份和载入配置，您可以进入下面的操作界面。配置备份功能可以将您路由器的设置以文件形式保存到电脑中，以备下次使用；配置载入功能则是将先前保存的或已编辑好的配置重新装入。配置界面如下:

配置文件备份与载入

您可以在这保存您的设置。我们建议您在修改配置及升级软件前备份您的配置文件。

备份配置文件

您可以通过载入配置文件来恢复您的设置。

路 径： 浏览... 载入配置文件

注意： 1. 载入配置文件后，设备中原有的用户配置将会丢失，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。
2. 载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。

帮 助

- **备份配置文件**: 将配置以文件形式保存。
- **路径**: 配置文件的全路径。

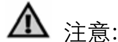
➢ **浏览**：选择配置文件。

➢ **载入配置文件**：装入先前保存的或已编辑好的配置文件。

典型用法：

➢ 升级软件或在载入新配置文件前备份原配置，以防止升级软件或载入新配置文件时操作有误，丢失配置。

➢ 为多台路由器配置相同的设置。先设置一台路由器，保存其配置文件后，再将它载入到其它的路由器中，以节省时间。


注意：

1 载入配置文件后，设备中原有的用户配置将会丢失，如果您需要保存原有配置，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。

2 载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重启。如果载入有错，请根据提示信息及生效的配置选择自己是否需要保存配置，然后最好再重启路由器。

例如：

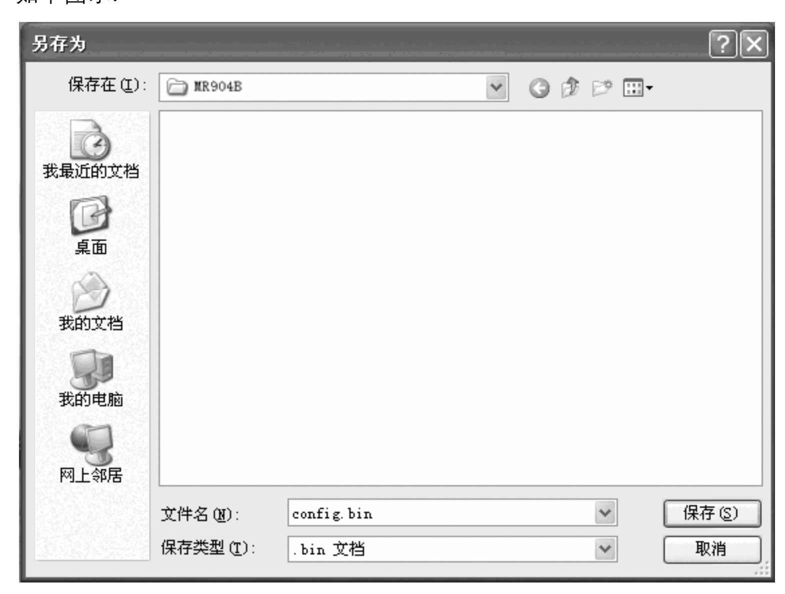
备份配置到：C:\Mercury\MR904B\config.bin；然后，将其载入到另一台路由器中。

备份配置步骤如下：

➢ 选择系统工具下的备份和载入配置项，单击备份配置文件按钮，出现下面操作界面：

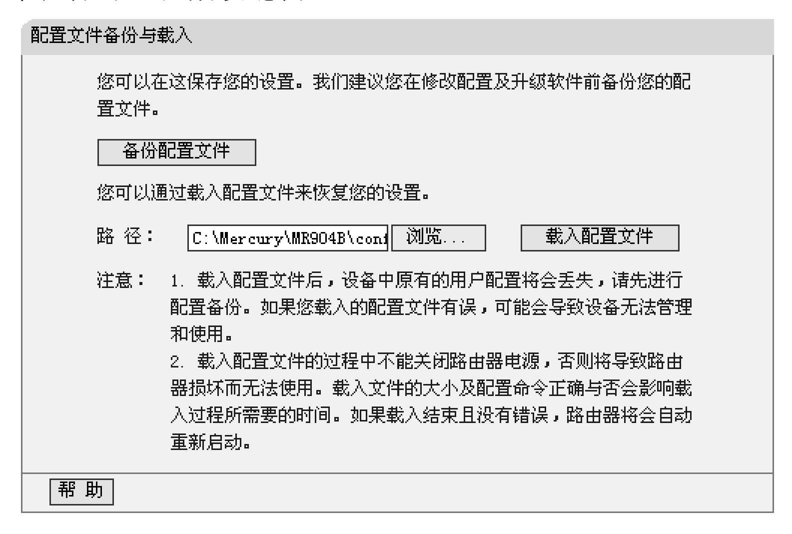


➢ 点击保存按钮，将配置文件config.bin保存在文件夹C:\Mercury\MR904B中。如下图示:



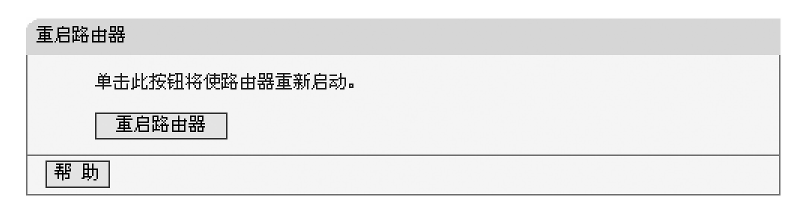
载入配置步骤如下:

➢ 更换另一台路由器，选择系统工具下的备份和载入配置项，输入载入文件夹的详细路径（如：C:\Mercury\MR904B\config.bin）或点击浏览按钮选择载入文件夹，然后单击载入配置文件按钮即可完成文件载入。下图为输入文件路径，载入配置文件的示意图。



5.14.5 重启路由器

选择系统工具下的重启路由器，您可以进入下面的操作界面。单击重启路由器按钮，路由器就会重新启动。操作界面显示如下:



5.14.6 修改登录口令

选择系统工具下的修改登录口令，您可以进入下面的操作界面。本页修改系统管理员的用户名及口令。修改界面如下:

修改登录口令

本页修改系统管理员的用户名及口令。

原用户名： admin

原口令： •••••

新用户名： llyy

新口令： •••••

确认新口令： •••••

保 存　清 空

修改步骤:

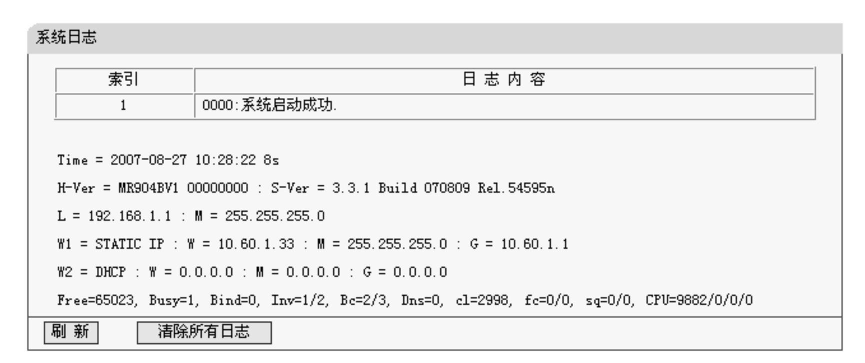
首先请您输入原来的用户名和口令，然后输入您希望使用的新用户名和口令。如果您原来的用户名和口令输入无误的话，单击“保存”即可成功修改用户名和口令。


注意:

出于安全考虑，我们强烈推荐您改变初始系统管理员用户名及密码。如果您忘了系统密码，请使用复位按钮恢复到出厂设置。

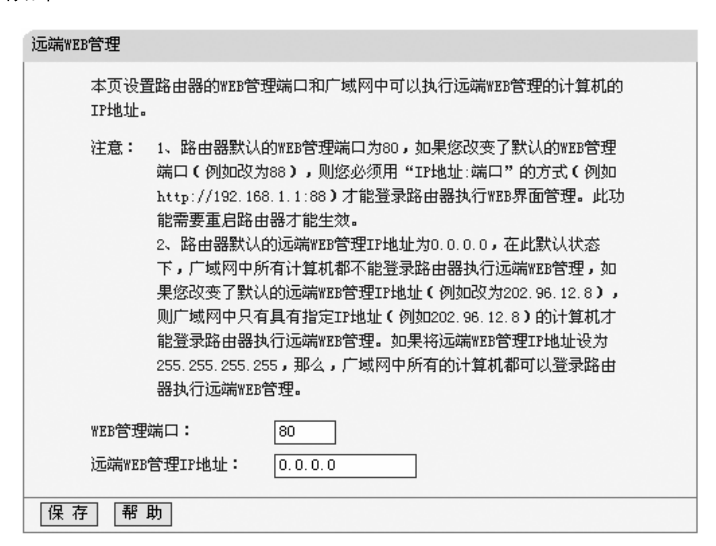
5.14.7 系统日志

选择系统工具下的系统日志，您可以进入下面的显示界面。该部分记录了路由器的系统日志，您可以通过查询日志了解路由器上发生的系统事件。界面显示如下:



5.14.8 远端 WEB 管理

选择系统工具下的远端WEB管理，您可以进入下面的操作界面。本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。设置界面如下:



➢ **WEB管理端口**: 可以执行WEB管理的端口号。

➢ **远端WEB管理IP地址**：广域网中可以执行远端WEB管理的计算机的IP地址。

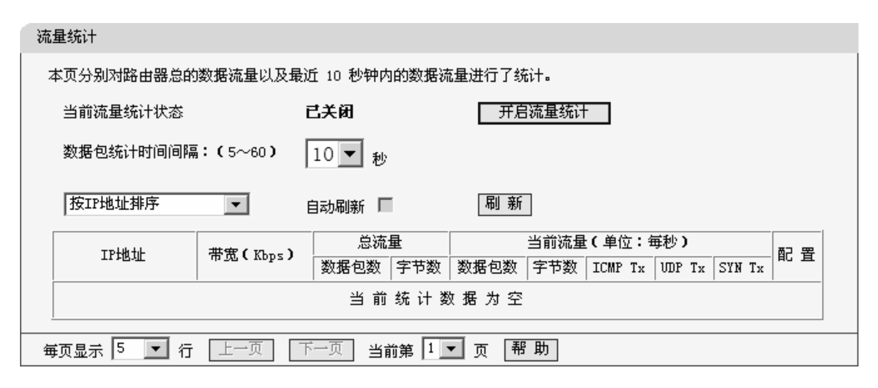
 注意：

1　路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口(例如改为88)，则您必须用“IP地址：端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才生效。若远端用户需要访问该管理页面，必须输入http://222.88.88.161:88（假设远端IP地址为222.88.88.161）。

2　路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB 管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。

5.14.9　流量统计

选择系统工具下的流量统计，您可以进入下面的操作界面。



➢ **当前流量统计状态**：请您选择是否需要开启流量统计，如无需进行流量统计，可点击关闭流量统计按钮禁用该功能，这样可提高路由器的数据处理能力。

➢ **数据包统计时间间隔**：请您选择当前统计流量的时间间隔。它与“安全设置”－“高级安全设置”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。

➢ **流量统计列表**：显示流量统计的信息。

- **IP地址**：显示被统计主机的IP地址。
- **带宽**：显示被统计主机10秒钟内收、发数据的字节数。
- **总流量**：显示当前数据的总流量，分别用数据包和字节数来衡量该值。
  - **数据包数**：路由器总的收、发数据包的个数。

   - **字节数:** 路由器收、发数据的总计字节数。
- **当前流量**: 显示当前设置的时间间隔内（图中为10秒）的数据流量。
   - **数据包数**: 路由器当前 10 秒钟内收、发数据包的个数。
   - **字节数**: 路由器当前 10 秒钟内收、发数据的字节数。
   - **ICMP Tx**: 路由器当前 10 秒钟内发送到广域网的ICMP包的个数。
   - **UDP Tx**: 路由器当前10秒钟内发送到广域网的UDP包的个数。
   - **TCP SYN Tx**: 路由器当前10秒钟内发送到广域网的TCP SYN包的个数。

➢ **每页显示:** 设置每页可以显示的最大条目数（默认值为5）。

➢ **上一页、下一页:** 单击该按钮，可以分别转入界面的上一页或下一页。

➢ **当前第 页:** 显示当前的页码。

5.14.10 联机测试

选择系统工具下的联机测试，您可以进入下面的操作界面。联机测试可以用来测试路由器的LAN口、WAN口1和WAN口2的端口速度，具体是通过计算路由器发送测试包至收到对方的应答包的时间间隔来衡量端口的速度。测试方法有ICMP检测、TCP检测以及UDP检测。联机测试的设置界面如下:

联机测试

被测端口： WAN口1

ICMP检测

目的IP：

标识符： 0

检测结果：

TCP检测

目的IP：

目的端口： 0

源端口： 0

检测结果：

UDP检测

目的IP：

目的端口： 0

源端口： 0

UDP数据：

检测结果：

注意：以上的UDP数据中，如果存在“.”字符，则该数据将被认为是一个域名，否则将被当作完整的UDP数据进行发送。

帮 助

- **被测端口:** 该项用来选择需要进行速度检测的端口。
- **ICMP检测:** 点击此按钮，对端口进行ICMP检测，并显示检测结果。
  - **目的IP**：请您输入ICMP包发往的目的地址。
  - **标识符**：请您输入ICMP包中用来填充标识符字段的值。
  - **检测结果:** 显示发送ICMP测试包至收到应答包之间的响应时间。
- **TCP检测:** 点击该按钮，对端口进行TCP检测，并显示检测结果。
  - **目的IP**：请您输入TCP包发往的目的地址。
  - **目的端口:** 请您输入TCP包发往的目的端口。
  - **源端口**：请您输入发送TCP包的源端口。
  - **检测结果:** 显示发送TCP测试包至收到应答包之间的响应时间。
- **UDP检测:** 点击该按钮，对端口进行UDP检测，并显示检测结果。

- **目的IP**：请您输入UDP包发往的目的地址。
- **目的端口**：请您输入UDP包发往的目的端口。
- **源端口**：请您输入发送UDP包的源端口。
- **UDP数据**：请您输入UDP测试包携带的数据。
- **检测结果**：显示发送UDP测试包至收到应答包之间的响应时间。


注意:

如果发送的UDP数据中含有字符“.”，如123.456，则认为该数据是一个域名，它将作为一个DSN查询包处理，而不作为UDP测试包处理。

5.14.11 IP 地址转换表

选择系统工具下的IP地址转换表，您可以进入下面的操作界面。IP地址转换表主要用于查看NAPT(网络地址端口转换)表中的信息。具体界面显示如下（图片只显示了部分地址内容）：

IP地址转换表

出口线路：WAN口1　协议类型：ALL　IP地址：192.168.1.193　显示　刷新

协议类型	本地IP地址	本地端口	转换端口	远端IP地址	远端端口	老化时间	出口线路
TCP	192.168.1.193	4330	1043	222.88.88.5	445	1775	WAN口1
TCP	192.168.1.193	4331	1044	222.88.88.5	139	4	WAN口1
TCP	192.168.1.193	4332	1045	222.88.88.25	445	1778	WAN口1
TCP	192.168.1.193	4333	1046	222.88.88.25	139	8	WAN口1

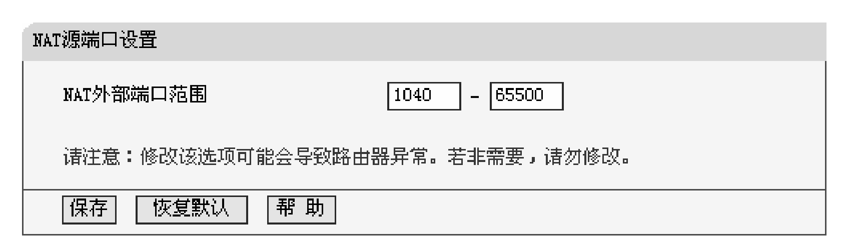
显示 20 行　帮 助

- **WAN口**：请您选择连接采用的端口类型，WAN口1、WAN口2或ALL。
- **协议类型**：请您输入WAN口建立连接时采用的协议类型。
- **IP地址**：请您输入需要查看的本地或远端主机的IP地址。
- **显示**：点击该按钮，您可以查看IP地址转换表信息。
- **刷新**：点击该按钮，您可以更新当前的IP地址转换表信息。
- **地址转换信息表**：显示地址转换表的详细信息。
  - **本地IP地址**：显示本地LAN端主机的IP地址。
  - **本地端口**：显示连接时，本地LAN端主机采用的端口号。
  - **转换端口**：显示数据包经NAT转换后，WAN口转发数据包中采用的源端口号。
  - **远程IP地址**：显示远端主机的IP地址。
  - **远程端口**：显示连接时，远端主机采用的端口号。
  - **老化时间**：显示当前连接可以维持的时间。

- **出口线路:** 显示当前连接所用的路由器的WAN端口号。

5.14.12 NAT 源端口设置

选择系统工具下的NAT源端口设置，您可以进入下面的操作界面。该项主要用来限制路由器进行NAT转换时采用的外部端口范围，具体设置界面如下:



➢ **NAT外部端口范围:** 请您输入需要限制的端口范围，系统默认值为10240－65534。

 注意:

该项默认值是经过系统测试确定的，修改该选项可能导致路由器工作异常，若非需要，请勿修改。

附录 A FAQ

1 ADSL 用户如何设置上网?

1) 首先，将 ADSL modem 设置为桥模式（RFC1483 桥模式）。
2) 用网线将路由器的 WAN 口与 ADSL modem 相连，电话线连 ADSL modem 的 Line 口。
3) 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“PPPoE”，输入“上网帐号”及“上网口令”，点击连接按钮即可。
4) 如果是包月上网的用户，可以选择“自动连接”的连接模式；如果是非包月用户，可以选择“按需连接”或者“手动连接”，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

2 LAN 接入的用户如何设置上网?

1) 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“动态 IP”，点击“保存”按钮即可。

2) 在某些网络服务商绑定了用户计算机网卡 MAC 地址的情况下，需要对路由器进行 MAC 地址克隆操作，将路由器的 WAN 口 MAC 地址设置为被绑定的网卡 MAC 地址。选择菜单“网络参数”下的“MAC 地址克隆”，在右边主窗口中点击“克隆 MAC 地址”按钮，然后按“保存”按钮，待路由器重启动后生效。

3 怎样使用 NetMeeting 聊天?

1) 如果是主动发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。

2) 如果希望能接收来自对方的 NetMeeting 呼叫，则需要设置虚拟服务器或 DMZ 主机。

3) 设置虚拟服务器方法：进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“1720”（NetMeeting 的连接端口），“IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.100），再在状态栏选择“生效”，点击“保存”按钮即可。如图:

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号：	1720	(XX-XX or XX)
IP地址：	192.168.1.100	
协议：	ALL	
状态：	生效	
常用服务端口号：	--请选择--	

保 存　返 回　帮 助

这样，对方呼叫您时只需输入您路由器 WAN 口的地址即可。

4) 设置 DMZ 主机方法：进入管理界面，选择菜单“转发规则”下的“DMZ 主机”，在“DMZ 主机 IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.101），再将“启用”选择框选中，点击“保存”按钮即可。如图:

DMZ主机

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。
（注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。）

DMZ 状态： ⦿启用 ○不启用

DMZ 主机IP地址： 192.168.1.101

保 存 帮 助

4 怎样在局域网构建 Web 服务器?

1) 在局域网构建服务器，只需要按问题 3 的第三点设置虚拟服务器即可。

2) 但在构建 Web 服务器时，Web 服务的服务端口与路由器本身 Web 管理界面的缺省端口相同，都是 80，这样就引起冲突。解决办法是修改路由器 Web 管理界面的端口。

3) 进入管理界面，选择菜单“系统工具”下的“远端 Web 管理”，在右边主窗口中，“Web 管理端口”栏输入 80 以外的值，如 88。点击保存并重启路由器。如图:

远端WEB管理

本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。

注意： 1、路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口（例如改为88），则您必须用“IP地址:端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才能生效。
2、路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。

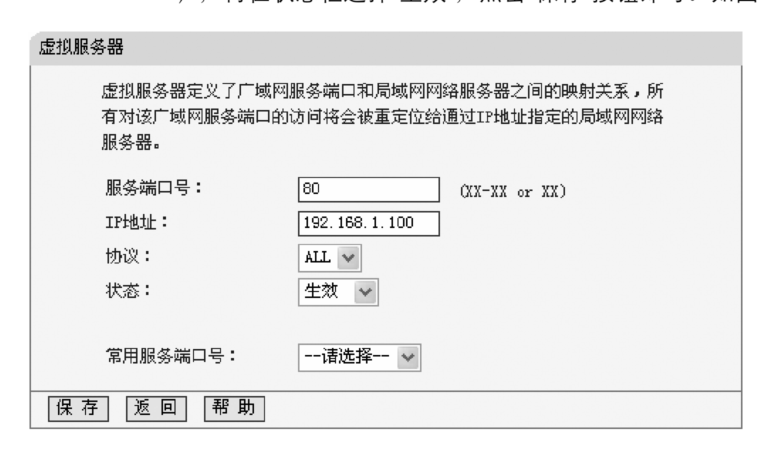
WEB管理端口： 88

远端WEB管理IP地址： 0.0.0.0

保 存 帮 助

4) 再次进入管理界面时，需要在浏览器的地址栏输入：http://192.168.1.1:88 才能进入。若远端用户需要访问该管理页面，必须输入 http://222.88.88.161:88（假设远端 IP 地址为 222.88.88.161）。

5) 进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“80”，这是 Web 服务器的连接端口，“IP 地址”栏填入 Web 服务器的 IP 地址（假设您的 Web 服务器的 IP 地址是 192.168.1.100），再在状态栏选择“生效”，点击“保存”按钮即可。如图:



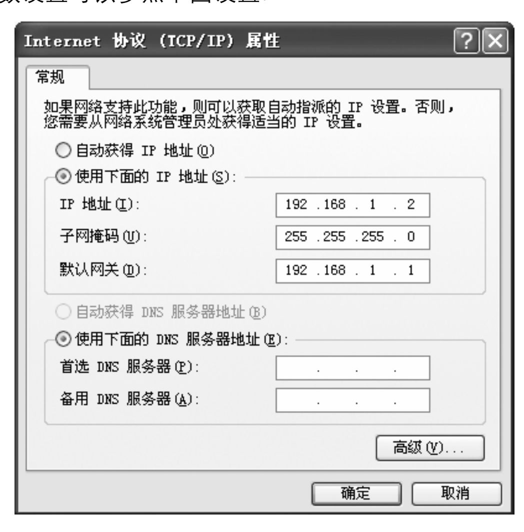
附录 B　TCP/IP 的详细设置

在这一节中将详细介绍TCP/IP的配置(本部分内容以Windows XP为例):

1 打开“开始→控制面板”中的“网络连接”，右键点击“本地连接”图标，单击“属性”选项，出现如下图所示页面:



2　双击“Internet 协议”（TCP/IP），出现如下图所示页面。如果您希望拥有固定的IP地址，请选择**使用下面的IP地址**和**使用下面的DNS服务器地址**，然后手动设置网络参数，其中IP地址为192.168.1.2－192.168.1.254范围内的任意值，参数设置可以参照下图设置:



3　如果您希望自动从路由器获得IP地址，请选择自动获得IP地址和自动获得DNS服务器地址，点击确定后设置将生效，如图示。

